Vulnerability Summary for the Week of April 19, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 04/26/2021 01:28 PM EDT

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of April 19, 2021

04/26/2021 07:37 AM EDT

Original release date: April 26, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- robohelp	Adobe Robohelp version 2020.0.3 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. An attacker with permissions to write to the file system could leverage this vulnerability to escalate privileges.	2021-04-19	9.3	CVE-2021-21070 MISC
autodesk -- fbx_review	A user may be tricked into opening a malicious FBX file which may exploit a Directory Traversal Remote Code Execution vulnerability in FBX's Review causing it to run arbitrary code on the system.	2021-04-19	9.3	CVE-2021-27030 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- fbx_review	A user may be tricked into opening a malicious FBX file which may exploit a use-after-free vulnerability in FBX's Review causing the application to reference a memory location controlled by an unauthorized third party, thereby running arbitrary code on the system.	2021-04-19	9.3	CVE-2021-27031 MISC MISC
canonical -- ubuntu_linux	The overlayfs implementation in the linux kernel did not properly validate with respect to user namespaces the setting of file capabilities on files in an underlying file system. Due to the combination of unprivileged user namespaces along with a patch carried in the Ubuntu kernel to allow unprivileged overlay mounts, an attacker could use this to gain elevated privileges.	2021-04-17	7.2	CVE-2021-3493 MISC MISC MISC
canonical -- ubuntu_linux	Shiftfs, an out-of-tree stacking file system included in Ubuntu Linux kernels, did not properly handle faults occurring during copy_from_user() correctly. These could lead to either a double-free situation or memory not being freed at all. An attacker could use this to cause a denial of service (kernel memory exhaustion) or gain privileges via executing arbitrary code. AKA ZDI-CAN-13562.	2021-04-17	7.2	CVE-2021-3492 MISC MISC MISC MISC MISC
cnesty -- helpcom	A vulnerability of Helpcom could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient authentication validation.	2021-04-20	7.5	CVE-2020-7856 MISC
ffmpegdotjs_project -- ffmpegdotjs	This affects all versions of package ffmpegdotjs. If attacker-controlled user input is given to the trimvideo function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23376 MISC MISC
fibaro -- home_center_2_firmware	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands as root user using a command injection vulnerability.	2021-04-19	9	CVE-2021-20991 CONFIRM FULLDISC MISC
fibaro -- home_center_2_firmware	In Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older an internal management service is accessible on port 8000 and some API endpoints could be accessed without authentication to trigger a shutdown, a reboot or a reboot into recovery mode.	2021-04-19	7.8	CVE-2021-20990 CONFIRM FULLDISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
killing_project -- killing	This affects all versions of package killing. If attacker-controlled user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23381 MISC MISC
lextudio -- restructuredtext	vscode-restructuredtext before 146.0.0 contains an incorrect access control vulnerability, where a crafted project folder could execute arbitrary binaries via crafted workspace configuration.	2021-04-20	7.5	CVE-2021-28793 MISC MISC MISC MISC
onion-oled-js_project -- onion-oled-js	This affects all versions of package onion-oled-js. If attacker-controlled user input is given to the scroll function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23377 MISC MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3. The componentStatus parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-04-19	7.5	CVE-2020-27240 MISC
openclinic_ga_project -- openclinic_ga	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3. The serialnumber parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2021-04-19	7.5	CVE-2020-27241 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- enterprise_manager	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected are 11.1.1.9 and 12.2.1.3 Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager for Fusion Middleware accessible data as well as unauthorized read access to a subset of Enterprise Manager for Fusion Middleware accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Enterprise Manager for Fusion Middleware. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2021-04-22	7.5	CVE-2021-2008 MISC
oracle -- secure_global_desktop	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Gateway). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	7.5	CVE-2021-2177 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Coherence Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-04-22	7.5	CVE-2021-2135 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-04-22	7.5	CVE-2021-2136 MISC
picotts_project -- picotts	This affects all versions of package picotts. If attacker-controlled user input is given to the say function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23378 MISC MISC
portkiller_project -- portkiller	This affects all versions of package portkiller. If (attacker-controlled) user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23379 MISC MISC
ps-visitor_project -- ps-visitor	This affects all versions of package ps-visitor. If attacker-controlled user input is given to the kill function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23374 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
psnode_project -- psnode	This affects all versions of package psnode. If attacker-controlled user input is given to the kill function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23375 MISC MISC
qnap -- qts	An SQL injection vulnerability has been reported to affect QNAP NAS running Multimedia Console or the Media Streaming add-on. If exploited, the vulnerability allows remote attackers to obtain application information. QNAP has already fixed this vulnerability in the following versions of Multimedia Console and the Media Streaming add-on. QTS 4.3.3: Media Streaming add-on 430.1.8.10 and later QTS 4.3.6: Media Streaming add-on 430.1.8.8 and later QTS 4.4.x and later: Multimedia Console 1.3.4 and later We have also fixed this vulnerability in the following versions of QTS 4.3.3 and QTS 4.3.6, respectively: QTS 4.3.3.1624 Build 20210416 or later QTS 4.3.6.1620 Build 20210322 or later	2021-04-17	7.5	CVE-2020-36195 MISC
qnap -- qts	A command injection vulnerability has been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 Build 20210202 and later QTS 4.5.1.1495 Build 20201123 and later QTS 4.3.6.1620 Build 20210322 and later QTS 4.3.4.1632 Build 20210324 and later QTS 4.3.3.1624 Build 20210416 and later QTS 4.2.6 Build 20210327 and later QuTS hero h4.5.1.1491 build 20201119 and later	2021-04-17	7.5	CVE-2020-2509 MISC
roar-pidusage_project -- roar-pidusage	This affects all versions of package roar-pidusage. If attacker-controlled user input is given to the stat function of this package on certain operating systems, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	2021-04-18	7.5	CVE-2021-23380 MISC MISC
rpm_spec_project -- rpm_spec	The unofficial vscode-rpm-spec extension before 0.3.2 for Visual Studio Code allows remote code execution via a crafted workspace configuration.	2021-04-16	7.5	CVE-2021-31414 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tendacn -- g0_firmware	Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input.	2021-04-16	10	CVE-2021-27691 MISC
tendacn -- g1_firmware	Command Injection in Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted "action/umountUSBPartition" request. This occurs because the "formSetUSBPartitionUmount" function executes the "doSystemCmd" function with untrusted input.	2021-04-16	10	CVE-2021-27692 MISC
wondercms -- wondercms	A remote code execution vulnerability in the installUpdateThemePluginAction function in index.php in WonderCMS 3.1.3, allows remote attackers to upload a custom plugin which can contain arbitrary code and obtain a webshell via the theme/plugin installer.	2021-04-20	7.5	CVE-2020-35314 MISC MISC MISC MISC
wondercms -- wondercms	A server-side request forgery (SSRF) vulnerability in the addCustomThemePluginRepository function in index.php in WonderCMS 3.1.3 allows remote attackers to execute arbitrary code via a crafted URL to the theme/plugin installer.	2021-04-20	7.5	CVE-2020-35313 MISC MISC MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- genuine_service	Adobe Genuine Service version 6.6 (and earlier) is affected by an Uncontrolled Search Path element vulnerability. An authenticated attacker could exploit this to to plant custom binaries and execute them with System permissions. Exploitation of this issue requires user interaction.	2021-04-16	6.9	CVE-2020-9667 MISC
adtran -- personal_phone_manager	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to multiple reflected cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.	2021-04-20	4.3	CVE-2021-25680 MISC MISC MISC
adtran -- personal_phone_manager	** UNSUPPORTED WHEN ASSIGNED ** AdTran Personal Phone Manager 10.8.1 software is vulnerable to an issue that allows for exfiltration of data over DNS. This could allow for exposed AdTran Personal Phone Manager web servers to be used as DNS redirectors to tunnel arbitrary data over DNS. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.	2021-04-20	5	CVE-2021-25681 MISC MISC MISC
alpinelinux -- apk-tools	In Alpine Linux apk-tools before 2.12.5, the tarball parser allows a buffer overflow and crash.	2021-04-21	5	CVE-2021-30139 MISC MISC
atlassian -- connect_express	Broken Authentication in Atlassian Connect Express (ACE) from version 3.0.2 before version 6.6.0: Atlassian Connect Express is a Node.js package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Express app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Express versions between 3.0.2 - 6.5.0 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.	2021-04-16	4	CVE-2021-26073 N/A MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- connect_spring_boot	Broken Authentication in Atlassian Connect Spring Boot (ACSB) from version 1.1.0 before version 2.1.3: Atlassian Connect Spring Boot is a Java Spring Boot package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Spring Boot app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Spring Boot versions between 1.1.0 - 2.1.2 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.	2021-04-16	4	CVE-2021-26074 N/A N/A
autodesk -- fbx_review	A Out-Of-Bounds Read/Write Vulnerability in Autodesk FBX Review version 1.4.0 may lead to remote code execution through maliciously crafted DLL files or information disclosure.	2021-04-19	6.8	CVE-2021-27027 MISC MISC MISC MISC MISC MISC
autodesk -- fbx_review	A Memory Corruption Vulnerability in Autodesk FBX Review version 1.4.0 may lead to remote code execution through maliciously crafted DLL files.	2021-04-19	6.8	CVE-2021-27028 MISC MISC MISC
autodesk -- fbx_review	The user may be tricked into opening a malicious FBX file which may exploit a Null Pointer Dereference vulnerability in FBX's Review causing the application to crash leading to a denial of service.	2021-04-19	4.3	CVE-2021-27029 MISC MISC
curveballjs -- a12n-server	a12n-server is an npm package which aims to provide a simple authentication system. A new HAL-Form was added to allow editing users in version 0.18.0. This feature should only have been accessible to admins. Unfortunately, privileges were incorrectly checked allowing any logged in user to make this change. Patched in v0.18.2.	2021-04-16	4	CVE-2021-29452 MISC CONFIRM
ezxml_project -- ezxml	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_parse_str() performs incorrect memory handling while parsing crafted XML files (out-of-bounds read after a certain strcspn failure).	2021-04-16	4.3	CVE-2021-31348 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ezxml_project -- ezxml	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_parse_str() performs incorrect memory handling while parsing crafted XML files (writing outside a memory region created by mmap).	2021-04-16	4.3	CVE-2021-31347 MISC
fibaro -- home_center_2_firmware	Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older initiate SSH connections to the Fibaro cloud to provide remote access and remote support capabilities. This connection can be intercepted using DNS spoofing attack and a device initiated remote port-forward channel can be used to connect to the web management interface. Knowledge of authorization credentials to the management interface is required to perform any further actions.	2021-04-19	4.3	CVE-2021-20989 CONFIRM FULLDISC MISC
fibaro -- home_center_2_firmware	In Fibaro Home Center 2 and Lite devices in all versions provide a web based management interface over unencrypted HTTP protocol. Communication between the user and the device can be eavesdropped to hijack sessions, tokens and passwords.	2021-04-19	5	CVE-2021-20992 CONFIRM FULLDISC MISC
google -- bazel	An attacker can place a crafted JSON config file into the project folder pointing to a custom executable. VScode-bazel allows the workspace path to lint *.bzl files to be set via this config file. As such the attacker is able to execute any executable on the system through vscode-bazel. We recommend upgrading to version 0.4.1 or above.	2021-04-16	6.8	CVE-2021-22539 MISC MISC
gpac -- gpac	There is a Null Pointer Dereference in function filter_core/filter_pck.c:gf_filter_pck_new_alloc_internal in GPAC 1.0.1. The pid comes from function av1dmx_parse_flush_sample, the ctx.opid maybe NULL. The result is a crash in gf_filter_pck_new_alloc_internal.	2021-04-19	4.3	CVE-2021-30015 MISC MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is heap-based buffer overflow in the function gp_rtp_builder_do_avc() in ietf/rtp_pck_mpeg4.c.	2021-04-21	6.8	CVE-2020-35979 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	An issue was discovered in gpac before 1.0.1. A NULL pointer dereference exists in the function dump_isom_sdp located in filedump.c. It allows an attacker to cause Denial of Service.	2021-04-21	4.3	CVE-2020-23932 MISC MISC
gpac -- gpac	There is a integer overflow in media_tools/av_parsers.c in the hevc_parse_slice_segment function in GPAC 1.0.1 which results in a crash.	2021-04-19	4.3	CVE-2021-30014 MISC MISC
gpac -- gpac	Memory leak in the stbl_GetSampleInfos function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	2021-04-19	4.3	CVE-2021-31256 MISC MISC
gpac -- gpac	In the adts_dmx_process function in filters/reframe_adts.c in GPAC 1.0.1, a crafted file may cause ctx->hdr.frame_size to be smaller than ctx->hdr.hdr_size, resulting in size to be a negative number and a heap overflow in the memcpy.	2021-04-19	4.3	CVE-2021-30019 MISC MISC
gpac -- gpac	In the function gf_hevc_read_pps_bs_internal function in media_tools/av_parsers.c in GPAC 1.0.1 there is a loop, which with crafted file, pps->num_tile_columns may be larger than sizeof(pps->column_width), which results in a heap overflow in the loop.	2021-04-19	4.3	CVE-2021-30020 MISC MISC
gpac -- gpac	There is a integer overflow in media_tools/av_parsers.c in the gf_avc_read_pps_bs_internal in GPAC 1.0.1. pps_id may be a negative number, so it will not return. However, avc->pps only has 255 unit, so there is an overflow, which results a crash.	2021-04-19	4.3	CVE-2021-30022 MISC MISC
gpac -- gpac	In filters/reframe_latm.c in GPAC 1.0.1 there is a Null Pointer Dereference, when gf_filter_pck_get_data is called. The first arg pck may be null with a crafted mp4 file,which results in a crash.	2021-04-19	4.3	CVE-2021-30199 MISC MISC
gpac -- gpac	The gf_isom_set_extraction_slc function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31258 MISC MISC
gpac -- gpac	The gf_isom_cenc_get_default_info_internal function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31259 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	The MergeTrack function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31260 MISC MISC
gpac -- gpac	The gf_hinter_track_new function in GPAC 1.0.1 allows attackers to read memory via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31261 MISC MISC
gpac -- gpac	The AV1_DuplicateConfig function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31262 MISC MISC
gpac -- gpac	The HintFile function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	2021-04-19	4.3	CVE-2021-31257 MISC MISC
gpac -- gpac	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function nhmldump_send_header located in write_nhml.c. It allows an attacker to cause Denial of Service.	2021-04-21	4.3	CVE-2020-23930 MISC MISC
gpac -- gpac	Buffer overflow in the tenc_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file, related invalid IV sizes.	2021-04-19	6.8	CVE-2021-31254 MISC MISC
gpac -- gpac	An issue was discovered in gpac before 1.0.1. The abst_box_read function in box_code_adobe.c has a heap-based buffer over-read.	2021-04-21	5.8	CVE-2020-23931 MISC MISC MISC
gpac -- gpac	Buffer overflow in the abst_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file.	2021-04-19	6.8	CVE-2021-31255 MISC MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is a use-after-free in the function gf_isom_box_del() in isomedia/box_funcs.c.	2021-04-21	6.8	CVE-2020-35980 MISC MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is an invalid pointer dereference in the function SetupWriters() in isomedia/isom_store.c.	2021-04-21	6.8	CVE-2020-35981 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 1.0.1. There is an invalid pointer dereference in the function gf_hinter_track_finalize() in media_tools/isom_hinter.c.	2021-04-21	6.8	CVE-2020-35982 MISC MISC
gpac -- gpac	An issue was discovered in gpac before 1.0.1. The abst_box_read function in box_code_adobe.c has a heap-based buffer over-read.	2021-04-21	5.8	CVE-2020-23928 MISC MISC MISC
gpac -- gpac	There is a integer overflow in function filter_core/filter_props.c:gf_props_assign_value in GPAC 1.0.1. In which, the arg const GF_PropertyValue *value,maybe value->value.data.size is a negative number. In result, memcpy in gf_props_assign_value failed.	2021-04-19	6.8	CVE-2021-29279 MISC MISC
hashicorp -- consul	HashiCorp Consul Enterprise version 1.8.0 up to 1.9.4 audit log can be bypassed by specifically crafted HTTP events. Fixed in 1.9.5, and 1.8.10.	2021-04-20	5	CVE-2021-28156 MISC MISC
hashicorp -- consul	HashiCorp Consul and Consul Enterprise up to version 1.9.4 key-value (KV) raw mode was vulnerable to cross-site scripting. Fixed in 1.9.5, 1.8.10 and 1.7.14.	2021-04-20	4.3	CVE-2020-25864 MISC MISC
ibm -- i	IBM i 7.1, 7.2, 7.3, and 7.4 SMTP allows a network attacker to send emails to non-existent local-domain recipients to the SMTP server, caused by using a non-default configuration. An attacker could exploit this vulnerability to consume unnecessary network bandwidth and disk space, and allow remote attackers to send spam email. IBM X-Force ID: 198056.	2021-04-21	6.4	CVE-2021-20501 XF CONFIRM
ibm -- resilient	IBM Resilient SOAR V38.0 could allow a privileged user to create create malicious scripts that could be executed as another user. IBM X-Force ID: 198759.	2021-04-19	6.5	CVE-2021-20527 CONFIRM XF
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196649.	2021-04-21	6.4	CVE-2021-20454 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server	IBM WebSphere Application Server 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196648.	2021-04-20	6.4	CVE-2021-20453 CONFIRM XF
innorix -- file_transfer_solution	Innorix Web-Based File Transfer Solution versuibs prior to and including 9.2.18.385 contains a vulnerability that could allow remote files to be downloaded and executed by setting the arguments to the internal method. A remote attacker could induce a user to access a crafted web page, causing damage such as malicious code infection.	2021-04-19	6.8	CVE-2020-7851 MISC MISC
jenkins -- config_file_provider	Jenkins Config File Provider Plugin 3.7.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2021-04-21	5.5	CVE-2021-21642 CONFIRM MLIST
jenkins -- config_file_provider	Jenkins Config File Provider Plugin 3.7.0 and earlier does not correctly perform permission checks in several HTTP endpoints, allowing attackers with global Job/Configure permission to enumerate system-scoped credentials IDs of credentials stored in Jenkins.	2021-04-21	4	CVE-2021-21643 CONFIRM MLIST
jose_project -- jose	jose-node-cjs-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	2021-04-16	4.3	CVE-2021-29446 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jose_project -- jose	jose-node-esm-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	2021-04-16	4.3	CVE-2021-29445 MISC CONFIRM
jose_project -- jose	jose is an npm library providing a number of cryptographic operations. In vulnerable versions AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. A possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). All major release versions have had a patch released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `^1.28.1 || ^2.0.5 || >=3.11.4`. Users should upgrade their v1.x dependency to ^1.28.1, their v2.x dependency to ^2.0.5, and their v3.x dependency to ^3.11.4. Thanks to Jason from Microsoft Vulnerability Research (MSVR) for bringing this up and Eva Sarafianou (@esarafianou) for helping to score this advisory.	2021-04-16	4.3	CVE-2021-29443 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jose_project -- jose	jose-browser-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	2021-04-16	4.3	CVE-2021-29444 CONFIRM MISC
manydesigns -- portofino	Portofino is an open source web development framework. Portofino before version 5.2.1 did not properly verify the signature of JSON Web Tokens. This allows forging a valid JWT. The issue will be patched in the upcoming 5.2.1 release.	2021-04-16	6.4	CVE-2021-29451 MISC CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It improperly handled account blocks for certain automatically created MediaWiki user accounts, thus allowing nefarious users to remain unblocked.	2021-04-22	5.5	CVE-2021-31554 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It incorrectly executed certain rules related to blocking accounts after account creation. Such rules would allow for user accounts to be created while blocking only the IP address used to create an account (and not the user account itself). Such rules could also be used by a nefarious, unprivileged user to catalog and enumerate any number of IP addresses related to these account creations.	2021-04-22	5.5	CVE-2021-31552 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mediawiki -- mediawiki	An issue was discovered in the CheckUser extension for MediaWiki through 1.35.2. MediaWiki usernames with trailing whitespace could be stored in the cu_log database table such that denial of service occurred for certain CheckUser extension pages and functionality. For example, the attacker could turn off Special:CheckUserLog and thus interfere with usage tracking.	2021-04-22	6.4	CVE-2021-31553 MISC MISC MISC MISC MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. A MediaWiki user who is partially blocked or was unsuccessfully blocked could bypass AbuseFilter and have their edits completed.	2021-04-22	4	CVE-2021-31548 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. Its AbuseFilterCheckMatch API reveals suppressed edits and usernames to unprivileged users through the iteration of crafted AbuseFilter rules.	2021-04-22	4	CVE-2021-31547 MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It incorrectly logged sensitive suppression deletions, which should not have been visible to users with access to view AbuseFilter log data.	2021-04-22	4	CVE-2021-31546 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the PageForms extension for MediaWiki through 1.35.2. Crafted payloads for Token-related query parameters allowed for XSS on certain PageForms-managed MediaWiki pages.	2021-04-22	4.3	CVE-2021-31551 MISC MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the CommentBox extension for MediaWiki through 1.35.2. Via crafted configuration variables, a malicious actor could introduce XSS payloads into various layers.	2021-04-22	4.3	CVE-2021-31550 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The Special:AbuseFilter/examine form allowed for the disclosure of suppressed MediaWiki usernames to unprivileged users.	2021-04-22	4	CVE-2021-31549 MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the Oauth extension for MediaWiki through 1.35.2. It did not validate the oarc_version (aka oauth_registered_consumer.oarc_version) parameter's length.	2021-04-22	5	CVE-2021-31555 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The page_recent_contributors leaked the existence of certain deleted MediaWiki usernames, related to rev_deleted.	2021-04-22	5	CVE-2021-31545 MISC MISC
mendix -- mendix	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.19), Mendix Applications using Mendix 8 (All versions < V8.17.0), Mendix Applications using Mendix 8 (V8.12) (All versions < V8.12.5), Mendix Applications using Mendix 8 (V8.6) (All versions < V8.6.9), Mendix Applications using Mendix 9 (All versions < V9.0.5). Authenticated, non-administrative users could modify their privileges by manipulating the user role under certain circumstances, allowing them to gain administrative privileges.	2021-04-16	6.5	CVE-2021-27394 CONFIRM
nvidia -- geforce_experience	NVIDIA GeForce Experience, all versions prior to 3.22, contains a vulnerability in GameStream plugins where log files are created using NT/System level permissions, which may lead to code execution, denial of service, or local privilege escalation.	2021-04-20	4.6	CVE-2021-1079 CONFIRM
omicronenergy -- stationguard	OMICRON StationGuard before 1.10 allows remote attackers to cause a denial of service (connectivity outage) via crafted tcp/20499 packets to the CTRL Ethernet port.	2021-04-20	5	CVE-2021-30464 CONFIRM MISC
oracle -- applications_framework	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Home page). The supported version that is affected is 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	6.4	CVE-2021-2200 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 5.5.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	4.9	CVE-2021-2191 MISC
oracle -- customers_online	Vulnerability in the Oracle Customers Online product of Oracle E-Business Suite (component: Customer Tab). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Customers Online. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Customers Online accessible data as well as unauthorized access to critical data or complete access to all Oracle Customers Online accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	5.5	CVE-2021-2156 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- database_server	Vulnerability in the Recovery component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA Level Account privilege with network access via Oracle Net to compromise Recovery. While the vulnerability is in Recovery, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Recovery accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	2021-04-22	4	CVE-2021-2173 MISC
oracle -- database_server	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any View, Select Any View privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2021-04-22	4	CVE-2021-2175 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- document_management_and_collaboration	Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Attachments). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Document Management and Collaboration. While the vulnerability is in Oracle Document Management and Collaboration, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Document Management and Collaboration accessible data as well as unauthorized update, insert or delete access to some of Oracle Document Management and Collaboration accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N).	2021-04-22	5.5	CVE-2021-2181 MISC
oracle -- email_center	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Email Center. While the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	2021-04-22	5.5	CVE-2021-2209 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- enterprise_manager	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected is 12.2.1.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Enterprise Manager for Fusion Middleware. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2134 MISC
oracle -- enterprise_manager_base_platform	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: UI Framework). The supported version that is affected is 13.4.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Enterprise Manager Base Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	5.8	CVE-2021-2053 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- financial_services_analytical_applications_infrastructure	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Rules Framework). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	5.8	CVE-2021-2140 MISC
oracle -- hyperion_financial_management	Vulnerability in the Hyperion Financial Management product of Oracle Hyperion (component: Task Automation). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion Financial Management. CVSS 3.1 Base Score 3.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L).	2021-04-22	4.6	CVE-2021-2158 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- internet_expenses	Vulnerability in the Oracle Internet Expenses product of Oracle E-Business Suite (component: Mobile Expenses). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Internet Expenses. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Internet Expenses accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2021-04-22	4.3	CVE-2021-2153 MISC
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2183 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2182 MISC
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2150 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2199 MISC
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2184 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2185 MISC
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2186 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2187 MISC
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2188 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- istore	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2197 MISC
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2198 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- marketing	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.7-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	6.4	CVE-2021-2205 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2201 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2202 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2215 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2203 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2208 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2212 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2213 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2196 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2230 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2217 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	4	CVE-2021-2226 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2193 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2278 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2293 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2298 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2299 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2300 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2021-04-22	4	CVE-2021-2301 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2305 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2021-04-22	4	CVE-2021-2308 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2194 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2178 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2180 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2172 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2170 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2169 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2164 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	4	CVE-2021-2179 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2021-04-22	5.5	CVE-2021-2304 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2021-04-22	4.3	CVE-2021-2155 MISC
oracle -- partner_management	Vulnerability in the Oracle Partner Management product of Oracle E-Business Suite (component: Attribute Admin Setup). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2195 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- peoplesoft_enterprise	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H).	2021-04-22	6.5	CVE-2021-2151 MISC
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Multichannel Framework). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	5.8	CVE-2021-2216 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- sales_offline	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Template). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	5	CVE-2021-2189 MISC
oracle -- sales_offline	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Template). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	5	CVE-2021-2190 MISC
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2021-04-22	4.6	CVE-2021-2167 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- trade_management	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2210 MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-04-22	5.8	CVE-2021-2206 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	4.4	CVE-2021-2145 MISC MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: TopLink Integration). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	5	CVE-2021-2157 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-04-22	5	CVE-2021-2204 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	4.3	CVE-2021-2211 MISC MISC
paloaltonetworks -- bridgecrew_checkov	An unsafe deserialization vulnerability in Bridgecrew Checkov by Prisma Cloud allows arbitrary code execution when processing a malicious terraform file. This issue impacts Checkov 2.0 versions earlier than Checkov 2.0.26. Checkov 1.0 versions are not impacted.	2021-04-20	6.5	CVE-2021-3035 MISC
paloaltonetworks -- globalprotect	A denial-of-service (DoS) vulnerability in Palo Alto Networks GlobalProtect app on Windows systems allows a limited Windows user to send specifically-crafted input to the GlobalProtect app that results in a Windows blue screen of death (BSOD) error. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.8; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.4.	2021-04-20	4.9	CVE-2021-3038 MISC
qnap -- quts_hero	A cross-site scripting (XSS) vulnerability has been reported to affect earlier versions of File Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 build 20210202 (and later) QTS 4.5.1.1456 build 20201015 (and later) QTS 4.3.6.1446 build 20200929 (and later) QTS 4.3.4.1463 build 20201006 (and later) QTS 4.3.3.1432 build 20201006 (and later) QTS 4.2.6 build 20210327 (and later) QuTS hero h4.5.1.1472 build 20201031 (and later) QuTScloud c4.5.4.1601 build 20210309 (and later) QuTScloud c4.5.3.1454 build 20201013 (and later)	2021-04-16	4.3	CVE-2018-19942 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sonicwall -- email_security	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to read an arbitrary file on the remote host.	2021-04-20	4	CVE-2021-20023 CONFIRM
tibco -- administrator	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a SQL injection attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.	2021-04-20	6.5	CVE-2021-28828 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tibco -- administrator	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a persistent CSV injection attack from the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.	2021-04-20	6	CVE-2021-28829 CONFIRM CONFIRM
tribalsystems -- zenario	SQL Injection in Tribalsystems Zenario CMS 8.8.52729 allows remote attackers to access the database or delete the plugin. This is accomplished via the `ID` input field of ajax.php in the `Pugin library - delete` module.	2021-04-16	6.4	CVE-2021-26830 CONFIRM
vmware -- nsx-t_data_center	VMware NSX-T contains a privilege escalation vulnerability due to an issue with RBAC (Role based access control) role assignment. Successful exploitation of this issue may allow attackers with local guest user account to assign privileges higher than their own permission level.	2021-04-19	4.6	CVE-2021-21981 MISC
xmbforum2 -- xmb	XMB is vulnerable to cross-site scripting (XSS) due to inadequate filtering of BBCode input. This bug affects all versions of XMB. All XMB installations must be updated to versions 1.9.12.03 or 1.9.11.16.	2021-04-19	4.3	CVE-2021-29399 MISC MISC MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adtran -- personal_phone_manager	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to an authenticated stored cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.	2021-04-20	3.5	CVE-2021-25679 MISC MISC MISC MISC
ibm -- spectrum_protect	IBM Spectrum Protect Server 7.1 and 8.1 is subject to a stack-based buffer overflow caused by improper bounds checking during the parsing of commands. By issuing such a command with an improper parameter, an authorized administrator could overflow a buffer and cause the server to crash. IBM X-Force ID: 197792.	2021-04-16	2.1	CVE-2021-20491 XF CONFIRM
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.11.x. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory. Specifically, for sequences of pointer arithmetic operations, the pointer modification performed by the first operation is not correctly accounted for when restricting subsequent operations.	2021-04-20	2.1	CVE-2021-29155 MISC MISC
mi -- miui	The application in the mobile phone can read the SNO information of the device, Xiaomi 10 MIUI < 2020.01.15.	2021-04-20	2.1	CVE-2020-14105 CONFIRM
online_discussion_forum_project -- online_discussion_forum	The messaging subsystem in the Online Discussion Forum 1.0 is vulnerable to XSS in the message body. An authenticated user can send messages to arbitrary users on the system that include javascript that will execute when viewing the messages page.	2021-04-19	3.5	CVE-2020-28141 EXPLOIT-DB

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	3.6	CVE-2021-2152 MISC
oracle -- database	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having RMAN executable privilege with logon to the infrastructure where Oracle Database - Enterprise Edition executes to compromise Oracle Database - Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition accessible data. CVSS 3.1 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2021-04-22	2.1	CVE-2021-2207 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- flexcube_direct_banking	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.2 and 12.0.3. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 2.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	2021-04-22	2.1	CVE-2021-2141 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2021-04-22	1.9	CVE-2021-2232 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	2021-04-22	3.3	CVE-2021-2307 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	3.5	CVE-2021-2171 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	3.5	CVE-2021-2174 MISC
oracle -- peoplesoft_enterprise_campus_software_campus_community	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Frameworks). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 3.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).	2021-04-22	3.5	CVE-2021-2159 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris as well as unauthorized update, insert or delete access to some of Oracle Solaris accessible data. Note: This vulnerability applies to Oracle Solaris on SPARC systems only. CVSS 3.1 Base Score 6.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).	2021-04-22	3.6	CVE-2021-2192 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	3.5	CVE-2021-2214 MISC
oracle -- zfs_storage_appliance	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	2021-04-22	1.9	CVE-2021-2149 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- zfs_storage_appliance	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Installation). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 1.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N).	2021-04-22	1.2	CVE-2021-2147 MISC
paloaltonetworks -- pan-os	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where secrets in PAN-OS XML API requests are logged in cleartext to the web server logs when the API is used incorrectly. This vulnerability applies only to PAN-OS appliances that are configured to use the PAN-OS XML API and exists only when a client includes a duplicate API parameter in API requests. Logged information includes the cleartext username, password, and API key of the administrator making the PAN-OS XML API request.	2021-04-20	2.1	CVE-2021-3036 MISC
paloaltonetworks -- pan-os	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where the connection details for a scheduled configuration export are logged in system logs. Logged information includes the cleartext username, password, and IP address used to export the PAN-OS configuration to the destination server.	2021-04-20	2.1	CVE-2021-3037 MISC
remoteclinic -- remote_clinic	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Chat" and "Personal Address" field on staff/register.php	2021-04-21	3.5	CVE-2021-31329 MISC
remoteclinic -- remote_clinic	Stored XSS in Remote Clinic v2.0 in /medicines due to Medicine Name Field.	2021-04-21	3.5	CVE-2021-31327 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
telegram -- telegram	The Telegram app 7.6.2 for iOS allows remote authenticated users to cause a denial of service (application crash) if the victim pastes an attacker-supplied message (e.g., in the Persian language) into a channel or group. The crash occurs in MtProtoKitFramework.	2021-04-20	3.5	CVE-2021-30496 MISC MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abus -- secvest_wireless_alarm_system	The ABUS Secvest wireless alarm system FUAA50000 (v3.01.17) fails to properly authenticate some requests to its built-in HTTPS interface. Someone can use this vulnerability to obtain sensitive information from the system, such as usernames and passwords. This information can then be used to reconfigure or disable the alarm system.	2021-04-21	not yet calculated	CVE-2020-28973 MISC
amazon -- freertos	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in stream_buffer.c for a stream buffer.	2021-04-22	not yet calculated	CVE-2021-31572 MISC MISC
amazon -- freertos	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in queue.c for queue creation.	2021-04-22	not yet calculated	CVE-2021-31571 MISC MISC
anysupport -- anysupport	AnySupport (Remote support solution) before 2019.3.21.0 allows directory traversing because of swprintf function to copy file from a management PC to a client PC. This can be lead to arbitrary file execution.	2021-04-22	not yet calculated	CVE-2020-7861 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- maven	Apache Maven will follow repositories that are defined in a dependency's Project Object Model (pom) which may be surprising to some users, resulting in potential risk if a malicious actor takes over that repository or is able to insert themselves into a position to pretend to be that repository. Maven is changing the default behavior in 3.8.1+ to no longer follow http (non-SSL) repository references by default. More details available in the referenced urls. If you are currently using a repository manager to govern the repositories used by your builds, you are unaffected by the risks present in the legacy behavior, and are unaffected by this vulnerability and change to default behavior. See this link for more information about repository management: https://maven.apache.org/repository-management.html	2021-04-23	not yet calculated	CVE-2021-26291 MISC MLIST MLIST MLIST MLIST
aquanplayer -- aquanplayer	There is a directory traversing vulnerability in the download page url of AquaNPlayer 2.0.0.92. The IP of the download page url is localhost and an attacker can traverse directories using "dot dot" sequences(../../) to view host file on the system. This vulnerability can cause information leakage.	2021-04-22	not yet calculated	CVE-2020-7858 CONFIRM
authelia -- authelia	Authelia is an open-source authentication and authorization server providing 2-factor authentication and single sign-on (SSO) for your applications via a web portal. In versions 4.27.4 and earlier, utilizing a HTTP query parameter an attacker is able to redirect users from the web application to any domain, including potentially malicious sites. This security issue does not directly impact the security of the web application itself. As a workaround, one can use a reverse proxy to strip the query parameter from the affected endpoint. There is a patch for version 4.28.0.	2021-04-21	not yet calculated	CVE-2021-29456 CONFIRM
automox_agent -- automox_agent	Automox Agent prior to version 31 uses an insufficiently protected S3 bucket endpoint for storing sensitive files, which could be brute-forced by an attacker to subvert an organization's security program. The issue has since been fixed in version 31 of the Automox Agent.	2021-04-23	not yet calculated	CVE-2021-26909 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
automox_agent -- automox_agent	Automox Agent prior to version 31 logs potentially sensitive information in local log files, which could be used by a locally-authenticated attacker to subvert an organization's security program. The issue has since been fixed in version 31 of the Automox Agent.	2021-04-23	not yet calculated	CVE-2021-26908 CONFIRM MISC
avaya -- aura_orchestration_designer	An XML External Entities (XXE)vulnerability in the web-based user interface of Avaya Aura Orchestration Designer could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Orchestration Designer includes all 7.x versions before 7.2.3.	2021-04-23	not yet calculated	CVE-2020-7035 CONFIRM
avaya -- session_border_conroller	A command injection vulnerability in Avaya Session Border Controller for Enterprise could allow an authenticated, remote attacker to send specially crafted messages and execute arbitrary commands with the affected system privileges. Affected versions of Avaya Session Border Controller for Enterprise include 7.x, 8.0 through 8.1.1.x	2021-04-23	not yet calculated	CVE-2020-7034 CONFIRM
aviatrix -- controller	Insecure File Permissions exist in Aviatrix Controller 5.3.1516. Several world writable files and directories were found in the controller resource. Note: All Aviatrix appliances are fully encrypted. This is an extra layer of security.	2021-04-21	not yet calculated	CVE-2020-27568 CONFIRM
aviatrix -- vpn_client	Arbitrary File Write exists in Aviatrix VPN Client 2.8.2 and earlier. The VPN service writes logs to a location that is world writable and can be leveraged to gain write access to any file on the system.	2021-04-21	not yet calculated	CVE-2020-27569 CONFIRM
bento4 -- bento4	An issue was discovered in Bento4 through v1.6.0-637. A NULL pointer dereference exists in the function AP4_StszAtom::GetSampleSize() located in Ap4StszAtom.cpp. It allows an attacker to cause Denial of Service.	2021-04-21	not yet calculated	CVE-2020-23912 MISC
callback_assist -- callback_assist	An XML External Entities (XXE)vulnerability in Callback Assist could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Callback Assist includes all 4.0.x versions before 4.7.1.1 Patch 7.	2021-04-23	not yet calculated	CVE-2020-7036 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
check_point_identity_agent -- check_point_identity_agent	A denial of service vulnerability was reported in Check Point Identity Agent before R81.018.0000, which could allow low privileged users to overwrite protected system files.	2021-04-22	not yet calculated	CVE-2021-30356 CONFIRM
cifs-utils -- cifs-utils	A flaw was found in cifs-utils in versions before 6.13. A user when mounting a krb5 CIFS file system from within a container can use Kerberos credentials of the host. The highest threat from this vulnerability is to data confidentiality and integrity.	2021-04-19	not yet calculated	CVE-2021-20208 MISC MISC
cpp-peglib -- cpp-peglib	An issue was discovered in cpp-peglib through v0.1.12. peg::resolve_escape_sequence() in peglib.h has a heap-based buffer over-read.	2021-04-21	not yet calculated	CVE-2020-23915 MISC MISC
cpp-peglib -- cpp-peglib	An issue was discovered in cpp-peglib through v0.1.12. A NULL pointer dereference exists in the peg::AstOptimizer::optimize() located in peglib.h. It allows an attacker to cause Denial of Service.	2021-04-21	not yet calculated	CVE-2020-23914 MISC MISC
cscape -- cscape	Cscape (All versions prior to 9.90 SP4) lacks proper validation of user-supplied data when parsing project files. This could lead to memory corruption. An attacker could leverage this vulnerability to execute code in the context of the current process.	2021-04-23	not yet calculated	CVE-2021-22678 MISC
cscape -- cscape	Cscape (All versions prior to 9.90 SP4) is configured by default to be installed for all users, which allows full permissions, including read/write access. This may allow unprivileged users to modify the binaries and configuration files and lead to local privilege escalation.	2021-04-23	not yet calculated	CVE-2021-22682 MISC
dart -- sdk	Bad validation logic in the Dart SDK versions prior to 2.12.3 allow an attacker to use an XSS attack via DOM clobbering. The validation logic in dart:html for creating DOM nodes from text did not sanitize properly when it came across template tags.	2021-04-22	not yet calculated	CVE-2021-22540 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
debian -- xscreensaver	The Debian xscreensaver 5.42+dfsg1-1 package for XScreenSaver has cap_net_raw enabled for the /usr/libexec/xscreensaver/sonar file, which allows local users to gain privileges because this is arguably incompatible with the design of the Mesa 3D Graphics library dependency.	2021-04-21	not yet calculated	CVE-2021-31523 MISC MLIST
dell -- powerscale_onefs	Dell PowerScale OneFS 8.1.0 - 9.1.0 contains an LDAP Provider inability to connect over TLSv1.2 vulnerability. It may make it easier to eavesdrop and decrypt such traffic for a malicious actor. Note: This does not affect clusters which are not relying on an LDAP server for the authentication provider.	2021-04-20	not yet calculated	CVE-2020-26197 MISC
dell -- powerscale_onefs	Dell PowerScale OneFS 8.1.0 - 9.1.0 contains a privilege escalation in SmartLock compliance mode that may allow compadmin to execute arbitrary commands as root.	2021-04-20	not yet calculated	CVE-2021-21526 MISC
directum -- directum	Settings.aspx?view=About in Directum 5.8.2 allows XSS via the HTTP User-Agent header.	2021-04-24	not yet calculated	CVE-2021-31794 MISC MISC
discord -- discord-recon	Discord-Recon is a bot for the Discord chat service. In versions of Discord-Recon 0.0.3 and prior, a remote attacker is able to read local files from the server that can disclose important information. As a workaround, a bot maintainer can locate the file `app.py` and add `.replace('..', '')` into the `Path` variable inside of the `recon` function. The vulnerability is patched in version 0.0.4.	2021-04-22	not yet calculated	CVE-2021-29466 CONFIRM
discord -- discord-recon	Discord-Recon is a bot for the Discord chat service. Versions of Discord-Recon 0.0.3 and prior contain a vulnerability in which a remote attacker is able to overwrite any file on the system with the command results. This can result in remote code execution when the user overwrite important files on the system. As a workaround, bot maintainers can edit their `setting.py` file then add `<` and `>` into the `RCE` variable inside of it to fix the issue without an update. The vulnerability is patched in version 0.0.4.	2021-04-22	not yet calculated	CVE-2021-29465 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
discord_recon -- discord_recon	### Impact - This issue could be exploited to read internal files from the system and write files into the system resulting in remote code execution ### Patches - This issue has been fixed on 0.0.3 version by adding a regex that validate if there's any arguments on the command. then disallow execution if there's an argument ### Workarounds - To fix this issue from your side, just upgrade discord-recon, if you're unable to do that. then just copy the code from `assets/CommandInjection.py` and overwrite your code with the new one. that's the only code required. ### Credits - All of the credits for finding these issues on discord-recon goes to Omar Badran. ### For more information If you have any questions or comments about this advisory: * Email us at [mdaif1332@gmail.com] (mailto:mdaif1332@gmail.com)	2021-04-20	not yet calculated	CVE-2021-29461 CONFIRM
django -- wagtail	Wagtail is a Django content management system. In affected versions of Wagtail, when saving the contents of a rich text field in the admin interface, Wagtail does not apply server-side checks to ensure that link URLs use a valid protocol. A malicious user with access to the admin interface could thus craft a POST request to publish content with `javascript:` URLs containing arbitrary code. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. See referenced GitHub advisory for additional details, including a workaround. Patched versions have been released as Wagtail 2.11.7 (for the LTS 2.11 branch) and Wagtail 2.12.4 (for the current 2.12 branch).	2021-04-19	not yet calculated	CVE-2021-29434 CONFIRM MISC
djvu -- exiftool	Improper neutralization of user data in the DjVu file format in ExifTool versions 7.44 and up allows arbitrary code execution when parsing the malicious image	2021-04-23	not yet calculated	CVE-2021-22204 MISC MISC CONFIRM
dotcms -- dotcms	Cross Site Scripting (XSS) in dotCMS v5.1.5 allows remote attackers to execute arbitrary code by injecting a malicious payload into the "Task Detail" comment window of the "/dotAdmin/#/c/workflow" component.	2021-04-23	not yet calculated	CVE-2020-17542 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eclipse -- jersey	Eclipse Jersey 2.28 to 2.33 and Eclipse Jersey 3.0.0 to 3.0.1 contains a local information disclosure vulnerability. This is due to the use of the File.createTempFile which creates a file inside of the system temporary directory with the permissions: -rw-r--r--. Thus the contents of this file are viewable by all other users locally on the system. As such, if the contents written is security sensitive, it can be disclosed to other local users.	2021-04-22	not yet calculated	CVE-2021-28168 CONFIRM CONFIRM
eclipse -- openj9	In Eclipse Openj9 to version 0.25.0, usage of the jdk.internal.reflect.ConstantPool API causes the JVM in some cases to pre-resolve certain constant pool entries. This allows a user to call static methods or access static members without running the class initialization method, and may allow a user to observe uninitialized values.	2021-04-21	not yet calculated	CVE-2021-28167 CONFIRM
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A heap buffer overflow was found in Exiv2 versions v0.27.3 and earlier. The heap overflow is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when _writing_ the metadata, which is a less frequently used Exiv2 operation than _reading_ the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `insert`. The bug is fixed in version v0.27.4.	2021-04-19	not yet calculated	CVE-2021-29457 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as insert. The bug is fixed in version v0.27.4.	2021-04-23	not yet calculated	CVE-2021-29470 CONFIRM MISC
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as insert. The bug is fixed in version v0.27.4.	2021-04-19	not yet calculated	CVE-2021-29458 MISC CONFIRM MISC
ezxml -- libezxml	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_decode() performs incorrect memory handling while parsing crafted XML files, leading to a heap-based buffer overflow.	2021-04-24	not yet calculated	CVE-2021-31598 MISC
fast_ber -- fast_ber	An issue was discovered in fast_ber through v0.4. yy::yylex() in asn_compiler.hpp has a heap-based buffer over-read.	2021-04-21	not yet calculated	CVE-2020-23921 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
feifeicms -- feifeicms	Path Traversal in FeiFeiCMS v4.0 allows remote attackers to delete arbitrary files by sending a crafted HTTP request to " /index.php?s=/admin-tpl-del&id=".	2021-04-22	not yet calculated	CVE-2020-17563 MISC
feifeicms -- feifeicms	Path Traversal in FeiFeiCMS v4.0 allows remote attackers to delete arbitrary files by sending a crafted HTTP request to the " Admin/DataAction.class.php" component.	2021-04-22	not yet calculated	CVE-2020-17564 MISC
fusionauth -- fusionauth	FusionAuth fusionauth-samlv2 before 0.5.4 allows XXE attacks via a forged AuthnRequest or LogoutRequest because parseFromBytes uses javax.xml.parsers.DocumentBuilderFactory unsafely.	2021-04-22	not yet calculated	CVE-2021-27736 MISC MISC MISC
get16u -- get16u	A heap-based buffer overflow was found in jhead in version 3.06 in Get16u() in exif.c when processing a crafted file.	2021-04-22	not yet calculated	CVE-2021-3496 MISC MISC
giflib -- giflib	An issue was discovered in giflib through 5.1.4. DumpScreen2RGB in gif2rgb.c has a heap-based buffer over-read.	2021-04-21	not yet calculated	CVE-2020-23922 MISC
gitlab -- ce/ee	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.	2021-04-23	not yet calculated	CVE-2021-22205 MISC MISC CONFIRM
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions starting with 12.9. GitLab was vulnerable to a stored XSS if scoped labels were used.	2021-04-22	not yet calculated	CVE-2021-22199 CONFIRM MISC MISC
grassroot_platform -- grassroot_platform	Grassroot Platform is an application to make it faster, cheaper and easier to persistently organize and mobilize people in low-income communities. Grassroot Platform before master deployment as of 2021-04-16 did not properly verify the signature of JSON Web Tokens when refreshing an existing JWT. This allows to forge a valid JWT. The problem has been patched in version 1.3.1 by deprecating the JWT refresh function, which was an overdue deprecation regardless (the "refresh" flow is no longer used).	2021-04-19	not yet calculated	CVE-2021-29455 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gstreamer -- gstreamer	GStreamer before 1.18.4 might cause heap corruption when parsing certain malformed Matroska files.	2021-04-19	not yet calculated	CVE-2021-3498 MISC MISC DEBIAN
gstreamer -- gstreamer	GStreamer before 1.18.4 might access already-freed memory in error code paths when demuxing certain malformed Matroska files.	2021-04-19	not yet calculated	CVE-2021-3497 MISC MISC DEBIAN
hardware_sentry -- km	In Hardware Sentry KM before 10.0.01 for BMC PATROL, a cleartext password may be discovered after a failure or timeout of a command.	2021-04-23	not yet calculated	CVE-2021-31791 MISC
hashicorp -- terraform_vault_provider	HashiCorp Terraform's Vault Provider (terraform-provider-vault) did not correctly configure GCE-type bound labels for Vault's GCP auth method. Fixed in 2.19.1.	2021-04-22	not yet calculated	CVE-2021-30476 CONFIRM MISC
hashicorp -- vault_and_vault_enterprise	HashiCorp Vault and Vault Enterprise Cassandra integrations (storage backend and database secrets engine plugin) did not validate TLS certificates when connecting to Cassandra clusters. Fixed in 1.6.4 and 1.7.1	2021-04-22	not yet calculated	CVE-2021-27400 CONFIRM
hashicorp -- vault_enterprise	HashiCorp Vault and Vault Enterprise 1.5.1 and newer, under certain circumstances, may exclude revoked but unexpired certificates from the CRL. Fixed in 1.5.8, 1.6.4, and 1.7.1.	2021-04-22	not yet calculated	CVE-2021-29653 CONFIRM
jenkins -- cloudbees_cd_plugin	Jenkins CloudBees CD Plugin 1.1.21 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Item/Read permission to schedule builds of projects without having Item/Build permission.	2021-04-21	not yet calculated	CVE-2021-21647 CONFIRM MLIST
jenkins -- confi_file_provider_plugin	Jenkins Config File Provider Plugin 3.7.0 and earlier does not perform permission checks in several HTTP endpoints, attackers with Overall/Read permission to enumerate configuration file IDs.	2021-04-21	not yet calculated	CVE-2021-21645 CONFIRM MLIST
jenkins -- confi_file_provider_plugin	A cross-site request forgery (CSRF) vulnerability in Jenkins Config File Provider Plugin 3.7.0 and earlier allows attackers to delete configuration files corresponding to an attacker-specified ID.	2021-04-21	not yet calculated	CVE-2021-21644 CONFIRM MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- templating_engine_plugin	Jenkins Templating Engine Plugin 2.1 and earlier does not protect its pipeline configurations using Script Security Plugin, allowing attackers with Job/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM.	2021-04-21	not yet calculated	CVE-2021-21646 CONFIRM MLIST
jtekt_corporation -- toyopuc_products	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.	2021-04-19	not yet calculated	CVE-2021-27458 MISC
juniper_networks -- appformix_agent	An unvalidated REST API in the AppFormix Agent of Juniper Networks AppFormix allows an unauthenticated remote attacker to execute commands as root on the host running the AppFormix Agent, when certain preconditions are performed by the attacker, thus granting the attacker full control over the environment. This issue affects: Juniper Networks AppFormix 3 versions prior to 3.1.22, 3.2.14, 3.3.0.	2021-04-22	not yet calculated	CVE-2021-0265 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	An Improper Input Validation vulnerability in the active-lease query portion in JDHCPD's DHCP Relay Agent of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending a crafted DHCP packet to the device thereby crashing the jdhcpd DHCP service. This is typically configured for Broadband Subscriber Sessions. Continued receipt and processing of this crafted packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. This issue does not affect Junos OS Evolved.	2021-04-22	not yet calculated	CVE-2021-0267 MISC MISC
juniper_networks -- junos_os	An improper authorization vulnerability in the Simple Network Management Protocol daemon (snmpd) service of Juniper Networks Junos OS leads an unauthenticated attacker being able to perform SNMP read actions, an Exposure of System Data to an Unauthorized Control Sphere, or write actions to OIDs that support write operations, against the device without authentication. This issue affects: Juniper Networks Junos OS: 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S6, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.	2021-04-22	not yet calculated	CVE-2021-0260 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.	2021-04-22	not yet calculated	CVE-2021-0264 MISC MISC
juniper_networks -- junos_os	The use of multiple hard-coded cryptographic keys in cSRX Series software in Juniper Networks Junos OS allows an attacker to take control of any instance of a cSRX deployment through device management services. This issue affects: Juniper Networks Junos OS on cSRX Series: All versions prior to 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2.	2021-04-22	not yet calculated	CVE-2021-0266 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in the forwarding of transit TCPv6 packets received on the Ethernet management interface of Juniper Networks Junos OS allows an attacker to trigger a kernel panic, leading to a Denial of Service (DoS). Continued receipt and processing of these transit packets will create a sustained Denial of Service (DoS) condition. This issue only occurs when TCPv6 packets are routed through the management interface. Other transit traffic, and traffic destined to the management interface, are unaffected by this vulnerability. This issue was introduced as part of a TCP Parallelization feature added in Junos OS 17.2, and affects systems with concurrent network stack enabled. This feature is enabled by default, but can be disabled (see WORKAROUND section below). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.	2021-04-22	not yet calculated	CVE-2021-0258 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	The improper handling of client-side parameters in J-Web of Juniper Networks Junos OS allows an attacker to perform a number of different malicious actions against a target device when a user is authenticated to J-Web. An attacker may be able to supersede existing parameters, including hardcoded parameters within the HTTP/S session, access and exploit variables, bypass web application firewall rules or input validation mechanisms, and otherwise alter and modify J-Web's normal behavior. An attacker may be able to transition victims to malicious web services, or exfiltrate sensitive information from otherwise secure web forms. This issue affects: Juniper Networks Junos OS: All versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2.	2021-04-22	not yet calculated	CVE-2021-0269 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.	2021-04-22	not yet calculated	CVE-2021-0270 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A kernel memory leak in QFX10002-32Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016 devices Flexible PIC Concentrators (FPCs) on Juniper Networks Junos OS allows an attacker to send genuine packets destined to the device to cause a Denial of Service (DoS) to the device. On QFX10002-32Q, QFX10002-60C, QFX10002-72Q devices the device will crash and restart. On QFX10008, QFX10016 devices, depending on the number of FPCs involved in an attack, one more more FPCs may crash and traffic through the device may be degraded in other ways, until the attack traffic stops. A reboot is required to restore service and clear the kernel memory. Continued receipt and processing of these genuine packets will create a sustained Denial of Service (DoS) condition. On QFX10008, QFX10016 devices, an indicator of compromise may be the existence of DCPFE core files. You can also monitor PFE memory utilization for incremental growth: user@qfx-RE:0% cprod -A fpc0 -c "show heap 0" | grep -i ke 0 3788a1b0 3221225048 2417120656 804104392 24 Kernel user@qfx-RE:0% cprod -A fpc0 -c "show heap 0" | grep -i ke 0 3788a1b0 3221225048 2332332200 888892848 27 Kernel This issue affects: Juniper Networks Junos OS on QFX10002-32Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016: 16.1 versions 16.1R1 and above prior to 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R3-S2; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2. This issue does not affect releases prior to Junos OS 16.1R1. This issue does not affect EX Series devices. This issue does not affect Junos OS Evolved.	2021-04-22	not yet calculated	CVE-2021-0272 MISC MISC
juniper_networks -- junos_os	An always-incorrect control flow implementation in the implicit filter terms of Juniper Networks Junos OS and Junos OS	2021-04-22	not yet calculated	CVE-2021-0273 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Evolved on ACX5800, EX9200 Series, MX10000 Series, MX240, MX480, MX960 devices with affected Trio line cards allows an attacker to exploit an interdependency in the PFE UCODE microcode of the Trio chipset with various line cards to cause packets destined to the devices interfaces to cause a Denial of Service (DoS) condition by looping the packet with an unreachable exit condition ('Infinite Loop'). To break this loop once it begins one side of the affected LT interfaces will need to be disabled. Once disabled, the condition will clear and the disabled LT interface can be reenabled. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue only affects LT-LT interfaces. Any other interfaces are not affected by this issue. This issue affects the following cards: MPCE Type 3 3D MPC4E 3D 32XGE MPC4E 3D 2CGE+8XGE EX9200 32x10G SFP EX9200-2C-8XS FPC Type 5-3D FPC Type 5-LSR EX9200 4x40G QSFP An Indicator of Compromise (IoC) can be seen by examining the traffic of the LT-LT interfaces for excessive traffic using the following command: monitor interface traffic Before loop impact: Interface: lt-2/0/0, Enabled, Link is Up Encapsulation: Logical-tunnel, Speed: 100000mbps Traffic statistics: Current delta Input bytes: 3759900268942 (1456 bps) [0] <---------- LT interface utilization is low Output bytes: 3759900344309 (1456 bps) [0] <---------- LT interface utilization is low After loop impact: Interface: lt-2/0/0, Enabled, Link is Up Encapsulation: Logical-tunnel, Speed: 100000mbps Traffic statistics: Current delta Input bytes: 3765160313129 (2158268368 bps) [5260044187] <---------- LT interface utilization is very high Output bytes: 3765160399522 (2158266440 bps) [5260055213] <---------- LT interface utilization is very high This issue affects: Juniper Networks Junos OS on ACX5800, EX9200 Series, MX10000 Series, MX240, MX480, MX960. Versions 15.1F6, 16.1R1, and later versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. This issue does not affect the MX10001. This issue does not affect Juniper Networks Junos OS versions prior to 15.1F6, 16.1R1. Juniper Networks Junos OS Evolved on ACX5800, EX9200 Series, MX10000 Series, MX240, MX480, MX960 19.4 versions prior to 19.4R2-EVO. This issue does not affect the MX10001.			
juniper_networks -- junos_os	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.	2021-04-22	not yet calculated	CVE-2021-0275 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	Due to a vulnerability in DDoS protection in Juniper Networks Junos OS and Junos OS Evolved on QFX5K Series switches in a VXLAN configuration, instability might be experienced in the underlay network as a consequence of exceeding the default ddos-protection aggregate threshold. If an attacker on a client device on the overlay network sends a high volume of specific, legitimate traffic in the overlay network, due to an improperly detected DDoS violation, the leaf might not process certain L2 traffic, sent by spines in the underlay network. Continued receipt and processing of the high volume traffic will sustain the Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on QFX5K Series: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S2, 20.3R2. Juniper Networks Junos OS Evolved on QFX5220: All versions prior to 20.3R2-EVO.	2021-04-22	not yet calculated	CVE-2021-0259 MISC
juniper_networks -- junos_os	A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected.	2021-04-22	not yet calculated	CVE-2021-0271 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2;	2021-04-22	not yet calculated	CVE-2021-0237 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: __default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.	2021-04-22	not yet calculated	CVE-2021-0247 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.	2021-04-22	not yet calculated	CVE-2021-0238 MISC
juniper_networks -- junos_os	In Juniper Networks Junos OS Evolved, receipt of a stream of specific genuine Layer 2 frames may cause the Advanced Forwarding Toolkit (AFT) manager process (Evo-aftmand), responsible for handling Route, Class-of-Service (CoS), Firewall operations within the packet forwarding engine (PFE) to crash and restart, leading to a Denial of Service (DoS) condition. By continuously sending this specific stream of genuine Layer 2 frames, an attacker can repeatedly crash the PFE, causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R1-EVO. This issue does not affect Junos OS versions.	2021-04-22	not yet calculated	CVE-2021-0239 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, the Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash if a malformed DHCPv6 packet is received, resulting in a restart of the daemon. The daemon automatically restarts without intervention, but continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects DHCPv6. DHCPv4 is not affected by this issue. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2.	2021-04-22	not yet calculated	CVE-2021-0240 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash with a core dump if a specific DHCPv6 packet is received, resulting in a restart of the daemon. The daemon automatically restarts without intervention, but continued receipt and processing of these specific packets will repeatedly crash the JDHCPD process and sustain the Denial of Service (DoS) condition. This issue only affects DHCPv6. DHCPv4 is not affected by this issue. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1, 19.3R3-S2; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2.	2021-04-22	not yet calculated	CVE-2021-0241 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability due to the improper handling of direct memory access (DMA) buffers on EX4300 switches on Juniper Networks Junos OS allows an attacker sending specific unicast frames to trigger a Denial of Service (DoS) condition by exhausting DMA buffers, causing the FPC to crash and the device to restart. The DMA buffer leak is seen when receiving these specific, valid unicast frames on an interface without Layer 2 Protocol Tunneling (L2PT) or dot1x configured. Interfaces with either L2PT or dot1x configured are not vulnerable to this issue. When this issue occurs, DMA buffer usage keeps increasing and the following error log messages may be observed: Apr 14 14:29:34.360 /kernel: pid 64476 (pfex_junos), uid 0: exited on signal 11 (core dumped) Apr 14 14:29:33.790 init: pfe-manager (PID 64476) terminated by signal number 11. Core dumped! The DMA buffers on the FPC can be monitored by the executing vty command 'show heap': ID Base Total(b) Free(b) Used(b) % Name -- -- -------- ---------- ---------- ---------- --- --------- -- 0 4a46000 268435456 238230496 30204960 11 Kernel 1 18a46000 67108864 17618536 49490328 73 Bcm_sdk 2 23737000 117440512 18414552 99025960 84 DMA buf <<<<< keeps increasing 3 2a737000 16777216 16777216 0 0 DMA desc This issue affects Juniper Networks Junos OS on the EX4300: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2.	2021-04-22	not yet calculated	CVE-2021-0242 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	Improper Handling of Unexpected Data in the firewall policer of Juniper Networks Junos OS on EX4300 switches allows matching traffic to exceed set policer limits, possibly leading to a limited Denial of Service (DoS) condition. When the firewall policer discard action fails on a Layer 2 port, it will allow traffic to pass even though it exceeds set policer limits. Traffic will not get discarded, and will be forwarded even though a policer discard action is configured. When the issue occurs, traffic is not discarded as desired, which can be observed by comparing the Input bytes with the Output bytes using the following command: user@junos> monitor interface traffic Interface Link Input bytes (bps) Output bytes (bps) ge-0/0/0 Up 37425422 (82616) 37425354 (82616) <<<< egress ge-0/0/1 Up 37425898 (82616) 37425354 (82616) <<<< ingress The expected output, with input and output counters differing, is shown below: Interface Link Input bytes (bps) Output bytes (bps) ge-0/0/0 Up 342420570 (54600) 342422760 (54600) <<<< egress ge-0/0/1 Up 517672120 (84000) 342420570 (54600) <<<< ingress This issue only affects IPv4 policing. IPv6 traffic and firewall policing actions are not affected by this issue. This issue affects Juniper Networks Junos OS on the EX4300: All versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2.	2021-04-22	not yet calculated	CVE-2021-0243 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to 20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1.	2021-04-22	not yet calculated	CVE-2021-0235 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in Juniper Networks Junos OS ACX500 Series, ACX4000 Series, may allow an attacker to cause a Denial of Service (DoS) by sending a high rate of specific packets to the device, resulting in a Forwarding Engine Board (FFEB) crash. Continued receipt of these packets will sustain the Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on ACX500 Series, ACX4000 Series: 17.4 versions prior to 17.4R3-S2.	2021-04-22	not yet calculated	CVE-2021-0233 MISC
juniper_networks -- junos_os	An authentication bypass vulnerability in the Juniper Networks Paragon Active Assurance Control Center may allow an attacker with specific information about the deployment to mimic an already registered Test Agent and access its configuration including associated inventory details. If the issue occurs, the affected Test Agent will not be able to connect to the Control Center. This issue affects Juniper Networks Paragon Active Assurance Control Center All versions prior to 2.35.6; 2.36 versions prior to 2.36.2.	2021-04-22	not yet calculated	CVE-2021-0232 MISC
juniper_networks -- junos_os	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.	2021-04-22	not yet calculated	CVE-2021-0231 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A Use of Hard-coded Credentials vulnerability in Juniper Networks Junos OS on Junos Fusion satellite devices allows an attacker who is local to the device to elevate their privileges and take control of the device. This issue affects: Juniper Networks Junos OS Junos Fusion Satellite Devices. 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3-S2; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10; 17.4 version 17.4R3 and later versions; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2; 20.1 versions prior to 20.1R1-S1, 20.1R2. This issue does not affected Junos OS releases prior to 16.1R1 or all 19.2R3 and 19.4R3 release versions.	2021-04-22	not yet calculated	CVE-2021-0245 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1.	2021-04-22	not yet calculated	CVE-2021-0246 MISC
juniper_networks -- junos_os	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT:	2021-04-22	not yet calculated	CVE-2021-0249 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	In segment routing traffic engineering (SRTE) environments where the BGP Monitoring Protocol (BMP) feature is enable, a vulnerability in the Routing Protocol Daemon (RPD) process of Juniper Networks Junos OS allows an attacker to send a specific crafted BGP update message causing the RPD service to core, creating a Denial of Service (DoS) Condition. Continued receipt and processing of this update message will create a sustained Denial of Service (DoS) condition. This issue affects IPv4 and IPv6 environments. This issue affects: Juniper Networks Junos OS 17.4 versions 17.4R1 and above prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2, This issue does not affect Junos OS releases prior to 17.4R1. This issue affects: Juniper Networks Junos OS Evolved 19.2-EVO versions prior to 19.2R2-EVO.	2021-04-22	not yet calculated	CVE-2021-0250 MISC
juniper_networks -- junos_os	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2;	2021-04-22	not yet calculated	CVE-2021-0227 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On Juniper Networks Junos OS Evolved devices, receipt of a specific IPv6 packet may cause an established IPv6 BGP session to terminate, creating a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue does not affect IPv4 BGP sessions. This issue affects IBGP or EBGP peer sessions with IPv6. This issue affects: Juniper Networks Junos OS Evolved: 19.4 versions prior to 19.4R2-S3-EVO; 20.1 versions prior to 20.1R2-S3-EVO; 20.2 versions prior to 20.2R2-S1-EVO; 20.3 versions prior to 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS releases.	2021-04-22	not yet calculated	CVE-2021-0226 MISC
juniper_networks -- junos_os	NFX Series devices using Juniper Networks Junos OS are susceptible to a local command execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series 17.2 version 17.2R1 and later versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S3; 19.2 version 19.1R2 and later versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S2. 19.4 versions 19.4R3 and above. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.	2021-04-22	not yet calculated	CVE-2021-0253 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	An Improper Check for Unusual or Exceptional Conditions in Juniper Networks Junos OS Evolved may cause the stateless firewall filter configuration which uses the action 'policer' in certain combinations with other options to not take effect. An administrator can use the following CLI command to see the failures with filter configuration: user@device> show log kfirewall-agent.log | match ERROR Jul 23 14:16:03 ERROR: filter not supported This issue affects Juniper Networks Junos OS Evolved: Versions 19.1R1-EVO and above prior to 20.3R1-S2-EVO, 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS.	2021-04-22	not yet calculated	CVE-2021-0225 MISC
juniper_networks -- junos_os	A sensitive information disclosure vulnerability in the mosquitto message broker of Juniper Networks Junos OS may allow a locally authenticated user with shell access the ability to read portions of sensitive files, such as the master.passwd file. Since mosquitto is shipped with setuid permissions enabled and is owned by the root user, this vulnerability may allow a local privileged user the ability to run mosquitto with root privileges and access sensitive information stored on the local filesystem. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S12, 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.3 versions prior to 18.3R3-S4; 19.1 versions prior to 19.1R3-S4; 19.3 versions prior to 19.3R3-S1, 19.3R3-S2; 19.4 versions prior to 19.4R2-S3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2, 20.2R3.	2021-04-22	not yet calculated	CVE-2021-0256 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A local privilege escalation vulnerability in ethtraceroute of Juniper Networks Junos OS may allow a locally authenticated user with shell access to escalate privileges and write to the local filesystem as root. ethtraceroute is shipped with setuid permissions enabled and is owned by the root user, allowing local users to run ethtraceroute with root privileges. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D240; 17.3 versions prior to 17.3R3-S11, 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1.	2021-04-22	not yet calculated	CVE-2021-0255 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	An uncontrolled resource consumption vulnerability in Message Queue Telemetry Transport (MQTT) server of Juniper Networks Junos OS allows an attacker to cause MQTT server to crash and restart leading to a Denial of Service (DoS) by sending a stream of specific packets. A Juniper Extension Toolkit (JET) application designed with a listening port uses the Message Queue Telemetry Transport (MQTT) protocol to connect to a mosquitto broker that is running on Junos OS to subscribe for events. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: 16.1R1 and later versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1.	2021-04-22	not yet calculated	CVE-2021-0229 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	Due to an improper check for unusual or exceptional conditions in Juniper Networks Junos OS and Junos OS Evolved the Routing Protocol Daemon (RPD) service, upon receipt of a specific matching BGP packet meeting a specific term in the flowspec configuration, crashes and restarts causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects only Multiprotocol BGP (MP-BGP) VPNv6 FlowSpec deployments. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. Juniper Networks Junos OS Evolved: All versions after 18.4R1-EVO prior to 20.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved versions prior to 18.4R1-EVO.	2021-04-22	not yet calculated	CVE-2021-0236 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding | match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding | match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.	2021-04-22	not yet calculated	CVE-2021-0230 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN-(Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief | match lacp This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;	2021-04-22	not yet calculated	CVE-2021-0228 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	Due to an improper Initialization vulnerability on Juniper Networks Junos OS QFX5100-96S devices with QFX 5e Series image installed, ddos-protection configuration changes will not take effect beyond the default DDoS (Distributed Denial of Service) settings when configured from the CLI. The DDoS protection (jddosd) daemon allows the device to continue to function while protecting the packet forwarding engine (PFE) during the DDoS attack. When this issue occurs, the default DDoS settings within the PFE apply, as CPU bound packets will be throttled and dropped in the PFE when the limits are exceeded. To check if the device has this issue, the administrator can execute the following command to monitor the status of DDoS protection: user@device> show ddos-protection protocols error: the ddos-protection subsystem is not running This issue affects only QFX5100-96S devices. No other products or platforms are affected by this issue. This issue affects: Juniper Networks Junos OS on QFX5100-96S: 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R3, 19.1R3-S4; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2;	2021-04-22	not yet calculated	CVE-2021-0234 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in the handling of internal resources necessary to bring up a large number of Layer 2 broadband remote access subscriber (BRAS) nodes in Juniper Networks Junos OS can cause the Access Node Control Protocol daemon (ANCPD) to crash and restart, leading to a Denial of Service (DoS) condition. Continued processing of spoofed subscriber nodes will create a sustained Denial of Service (DoS) condition. When the number of subscribers attempting to connect exceeds the configured maximum-discovery-table-entries value, the subscriber fails to map to an internal neighbor entry, causing the ANCPD process to crash. This issue affects Juniper Networks Junos OS: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R2.	2021-04-22	not yet calculated	CVE-2021-0224 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in Juniper Networks Junos OS running on the ACX5448 and ACX710 platforms may cause BFD sessions to flap when a high rate of transit ARP packets are received. This, in turn, may impact routing protocols and network stability, leading to a Denial of Service (DoS) condition. When a high rate of transit ARP packets are exceptioned to the CPU and BFD flaps, the following log messages may be seen: bfdd[15864]: BFDD_STATE_UP_TO_DOWN: BFD Session 192.168.14.3 (IFL 232) state Up -> Down LD/RD(17/19) Up time:11:38:17 Local diag: CtlExpire Remote diag: None Reason: Detect Timer Expiry. bfdd[15864]: BFDD_TRAP_SHOP_STATE_DOWN: local discriminator: 17, new state: down, interface: irb.998, peer addr: 192.168.14.3 rpd[15839]: RPD_ISIS_ADJDOWN: IS-IS lost L2 adjacency to peer on irb.998, reason: BFD Session Down bfdd[15864]: BFDD_TRAP_SHOP_STATE_UP: local discriminator: 17, new state: up, interface: irb.998, peer addr: 192.168.14.3 This issue only affects the ACX5448 Series and ACX710 Series routers. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 18.2 versions prior to 18.2R3-S8 on ACX5448; 18.3 versions prior to 18.3R3-S5 on ACX5448; 18.4 versions prior to 18.4R1-S6, 18.4R3-S7 on ACX5448; 19.1 versions prior to 19.1R3-S5 on ACX5448; 19.2 versions prior to 19.2R2, 19.2R3 on ACX5448; 19.3 versions prior to 19.3R3 on ACX5448; 19.4 versions prior to 19.4R3 on ACX5448; 20.1 versions prior to 20.1R2 on ACX5448; 20.2 versions prior to 20.2R2 on ACX5448 and ACX710.	2021-04-22	not yet calculated	CVE-2021-0216 MISC
juniper_networks -- junos_os	On Juniper Networks MX Series and EX9200 Series platforms with Trio-based MPCs (Modular Port Concentrators) where Integrated Routing and Bridging (IRB) interfaces are configured and mapped to a VPLS instance or a Bridge-Domain, certain Layer 2 network events at Customer Edge (CE) devices may cause memory leaks in the MPC of Provider Edge (PE) devices which can cause an out of memory	2021-04-22	not yet calculated	CVE-2021-0257 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	condition and MPC restart. When this issue occurs, there will be temporary traffic interruption until the MPC is restored. An administrator can use the following CLI command to monitor the status of memory usage level of the MPC: user@device> show system resource-monitor fpc FPC Resource Usage Summary Free Heap Mem Watermark : 20 % Free NH Mem Watermark : 20 % Free Filter Mem Watermark : 20 % * - Watermark reached Slot # % Heap Free RTT Average RTT 1 87 PFE # % ENCAP mem Free % NH mem Free % FW mem Free 0 NA 88 99 1 NA 89 99 When the issue is occurring, the value of “% NH mem Free” will go down until the MPC restarts. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines), including MX-MPC1-3D, MX-MPC1E-3D, MX-MPC2-3D, MX-MPC2E-3D, MPC-3D-16XGE, and CHAS-MXxx Series MPCs. No other products or platforms are affected by this issue. This issue affects Juniper Networks Junos OS on MX Series, EX9200 Series: 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S3; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.2 versions prior to 20.2R1-S3, 20.2R2; 20.3 versions prior to 20.3R1-S1,, 20.3R2. This issue does not affect Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R3-S2; 18.1; 18.2 versions prior to 18.2R3-S4; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R3-S1; 19.1; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2.			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in the distributed or centralized periodic packet management daemon (PPMD) of Juniper Networks Junos OS may cause receipt of a malformed packet to crash and restart the PPMD process, leading to network destabilization, service interruption, and a Denial of Service (DoS) condition. Continued receipt and processing of these malformed packets will repeatedly crash the PPMD process and sustain the Denial of Service (DoS) condition. Due to the nature of the specifically crafted packet, exploitation of this issue requires direct, adjacent connectivity to the vulnerable component. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S12, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S5, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.	2021-04-22	not yet calculated	CVE-2021-0214 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') weakness in J-web of Juniper Networks Junos OS leads to buffer overflows, segment faults, or other impacts, which allows an attacker to modify the integrity of the device and exfiltration information from the device without authentication. The weakness can be exploited to facilitate cross-site scripting (XSS), cookie manipulation (modifying session cookies, stealing cookies) and more. This weakness can also be exploited by directing a user to a seemingly legitimate link from the affected site. The attacker requires no special access or permissions to the device to carry out such attacks. This issue affects: Juniper Networks Junos OS: 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S3; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.1R1.	2021-04-22	not yet calculated	CVE-2021-0268 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmand) process thereby denying users the ability to login, while concurrently impacting other mspmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.	2021-04-22	not yet calculated	CVE-2021-0251 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A vulnerability in the HTTP/HTTPS service used by J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through with Web-Redirect, and Captive Portal allows an unauthenticated attacker to cause an extended Denial of Service (DoS) for these services by sending a high number of specific requests. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S17 on EX Series; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 15.1 versions prior to 15.1R7-S8; 15.1X49 versions prior to 15.1X49-D230 on SRX Series; 16.1 versions prior to 16.1R7-S8; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2.	2021-04-22	not yet calculated	CVE-2021-0261 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages | grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.	2021-04-22	not yet calculated	CVE-2021-0244 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	Through routine static code analysis of the Juniper Networks Junos OS software codebase, the Secure Development Life Cycle team identified a Use After Free vulnerability in PFE packet processing on the QFX10002-60C switching platform. Exploitation of this vulnerability may allow a logically adjacent attacker to trigger a Denial of Service (DoS). Continued exploitation of this vulnerability will sustain the Denial of Service (DoS) condition. This issue only affects QFX10002-60C devices. No other product or platform is vulnerable to this issue. This issue affects Juniper Networks Junos OS on QFX10002-60C: 19.1 version 19.1R3-S1 and later versions; 19.1 versions prior to 19.1R3-S3; 19.2 version 19.2R2 and later versions; 19.2 versions prior to 19.2R3-S1; 20.2 versions prior to 20.2R1-S2. This issue does not affect Juniper Networks Junos OS: versions prior to 19.1R3; 19.2 versions prior to 19.2R2; any version of 19.3; version 20.2R2 and later releases.	2021-04-22	not yet calculated	CVE-2021-0262 MISC
juniper_networks -- junos_os	A Data Processing vulnerability in the Multi-Service process (multi-svcs) on the FPC of Juniper Networks Junos OS on the PTX Series routers may lead to the process becoming unresponsive, ultimately affecting traffic forwarding, allowing an attacker to cause a Denial of Service (DoS) condition . The Multi-Service Process running on the FPC is responsible for handling sampling-related operations when a J-Flow configuration is activated. This can occur during periods of heavy route churn, causing the Multi-Service Process to stop processing updates, without consuming any further updates from kernel. This back pressure towards the kernel affects further dynamic updates from other processes in the system, including RPD, causing a KRT-STUCK condition and traffic forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. The following logs/alarms will be observed when this condition exists: user@junos> show	2021-04-22	not yet calculated	CVE-2021-0263 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	chassis alarms 2 alarms currently active Alarm time Class Description 2020-10-11 04:33:45 PDT Minor Potential slow peers are: MSP(FPC1-PIC0) MSP(FPC3-PIC0) MSP(FPC4-PIC0) Logs: Oct 11 04:33:44.672 2020 test /kernel: rts_peer_cp_recv_timeout : Bit set for msp8 as it is stuck Oct 11 04:35:56.000 2020 test-lab fpc4 user.err gldfpc-multi-svcs.elf: Error in parsing composite nexthop Oct 11 04:35:56.000 2020 test-lab fpc4 user.err gldfpc-multi-svcs.elf: composite nexthop parsing error Oct 11 04:43:05 2020 test /kernel: rt_pfe_veto: Possible slowest client is msp38. States processed - 65865741. States to be processed - 0 Oct 11 04:55:55 2020 test /kernel: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (8311787520) Current delayed unref = (60000), Current unique delayed unref = (10896), Max delayed unref on this platform = (40000) Current delayed weight unref = (71426) Max delayed weight unref on this platform= (400000) curproc = rpd Oct 11 04:56:00 2020 test /kernel: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 This issue only affects PTX Series devices. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS on PTX Series: 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S8, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.2R1.			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	A buffer size validation vulnerability in the overlayd service of Juniper Networks Junos OS may allow an unauthenticated remote attacker to send specially crafted packets to the device, triggering a partial Denial of Service (DoS) condition, or leading to remote code execution (RCE). Continued receipt and processing of these packets will sustain the partial DoS. The overlayd daemon handles Overlay OAM packets, such as ping and traceroute, sent to the overlay. The service runs as root by default and listens for UDP connections on port 4789. This issue results from improper buffer size validation, which can lead to a buffer overflow. Unauthenticated attackers can send specially crafted packets to trigger this vulnerability, resulting in possible remote code execution. overlayd runs by default in MX Series, ACX Series, and QFX Series platforms. The SRX Series does not support VXLAN and is therefore not vulnerable to this issue. Other platforms are also vulnerable if a Virtual Extensible LAN (VXLAN) overlay network is configured. This issue affects Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1.	2021-04-22	not yet calculated	CVE-2021-0254 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper_networks -- junos_os	NFX Series devices using Juniper Networks Junos OS are susceptible to a local code execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series: 18.1 version 18.1R1 and later versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. This issue does not affect: Juniper Networks Junos OS versions prior to 18.1R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.	2021-04-22	not yet calculated	CVE-2021-0252 MISC
juniper_networks -- junos_os	This issue is not applicable to NFX NextGen Software. On NFX Series devices the use of Hard-coded Credentials in Juniper Networks Junos OS allows an attacker to take over any instance of an NFX deployment. This issue is only exploitable through administrative interfaces. This issue affects: Juniper Networks Junos OS versions prior to 19.1R1 on NFX Series. No other platforms besides NFX Series devices are affected.	2021-04-22	not yet calculated	CVE-2021-0248 MISC
libtpms -- lintpms	A flaw was found in libtpms in versions before 0.8.0. The TPM 2 implementation returns 2048 bit keys with ~1984 bit strength due to a bug in the TCG specification. The bug is in the key creation algorithm in RsaAdjustPrimeCandidate(), which is called before the prime number check. The highest threat from this vulnerability is to data confidentiality.	2021-04-19	not yet calculated	CVE-2021-3505 MISC MISC
linux -- linux_kernel	An out-of-bounds (OOB) memory access flaw was found in fs/f2fs/node.c in the f2fs module in the Linux kernel in versions before 5.12.0-rc4. A bounds check failure allows a local attacker to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability.	2021-04-19	not yet calculated	CVE-2021-3506 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	The PowerVR GPU kernel driver in pvrsrvkm.ko through 2021-04-24 for the Linux kernel, as used on Alcatel 1S phones, allows attackers to overwrite heap memory via PhysmemNewRamBackedPMR.	2021-04-24	not yet calculated	CVE-2021-31795 MISC
linux -- linux_kernel	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) before 5.12-rc8 can lead to kernel privilege escalation from the context of a network service or an unprivileged process. If sctp_destroy_sock is called without sock_net(sk)->sctp.addr_wq_lock then an element is removed from the auto_asconf_splist list without any proper locking. This can be exploited by an attacker with network service privileges to escalate to root or from the context of an unprivileged user directly if a BPF_CGROUP_INET_SOCK_CREATE is attached which denies creation of some SCTP socket.	2021-04-22	not yet calculated	CVE-2021-23133 CONFIRM CONFIRM
logo! -- logo!	A vulnerability has been identified in LOGO! Soft Comfort (All versions). The software insecurely loads libraries which makes it vulnerable to DLL hijacking. Successful exploitation by a local attacker could lead to a takeover of the system where the software is installed.	2021-04-22	not yet calculated	CVE-2020-25244 MISC
logo! -- logo!	A vulnerability has been identified in LOGO! Soft Comfort (All versions). A zip slip vulnerability could be triggered while importing a compromised project file to the affected software. Chained with other vulnerabilities this vulnerability could ultimately lead to a system takeover by an attacker.	2021-04-22	not yet calculated	CVE-2020-25243 MISC
magento -- magento-its	Magento-lts is a long-term support alternative to Magento Community Edition (CE). In magento-lts versions 19.4.12 and prior and 20.0.8 and prior, there is a vulnerability caused by the unsecured deserialization of an object. A patch in versions 19.4.13 and 20.0.9 was back ported from Zend Framework 3. The vulnerability was assigned CVE-2021-3007 in Zend Framework.	2021-04-21	not yet calculated	CVE-2021-21426 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
magento -- magento-its	Magento-lts is a long-term support alternative to Magento Community Edition (CE). A vulnerability in magento-lts versions before 19.4.13 and 20.0.9 potentially allows an administrator unauthorized access to restricted resources. This is a backport of CVE-2021-21024. The vulnerability is patched in versions 19.4.13 and 20.0.9.	2021-04-21	not yet calculated	CVE-2021-21427 CONFIRM
matrix-media-repo -- matrix-media-repo	matrix-media-repo is an open-source multi-domain media repository for Matrix. Versions 1.2.6 and earlier of matrix-media-repo do not properly handle malicious images which are crafted to be small in file size, but large in complexity. A malicious user could upload a relatively small image in terms of file size, using particular image formats, which expands to have extremely large dimensions during the process of thumbnailing. The server can be exhausted of memory in the process of trying to load the whole image into memory for thumbnailing, leading to denial of service. Version 1.2.7 has a fix for the vulnerability.	2021-04-19	not yet calculated	CVE-2021-29453 MISC MISC CONFIRM
metasploit -- metasploit	By launching the drb_remote_codeexec exploit, a Metasploit Framework user will inadvertently expose Metasploit to the same deserialization issue that is exploited by that module, due to the reliance on the vulnerable Distributed Ruby class functions. Since Metasploit Framework typically runs with elevated privileges, this can lead to a system compromise on the Metasploit workstation. Note that an attacker would have to lie in wait and entice the Metasploit user to run the affected module against a malicious endpoint in a "hack-back" type of attack. Metasploit is only vulnerable when the drb_remote_codeexec module is running. In most cases, this cannot happen automatically.	2021-04-23	not yet calculated	CVE-2020-7385 CONFIRM MISC MISC
misp -- misp	In app/Model/MispObject.php in MISP 2.4.141, an incorrect sharing group association could lead to information disclosure on an event edit. When an object has a sharing group associated with an event edit, the sharing group object is ignored and instead the passed local ID is reused.	2021-04-23	not yet calculated	CVE-2021-31780 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mitsubishi_electric_corporation -- multiple_products	Improper authentication vulnerability in GOT2000 series GT27 model all versions, GOT2000 series GT25 model all versions, GOT2000 series GT21 model GT2107-WTBD all versions ,GOT2000 series GT21 model GT2107-WTSD all versions, GOT SIMPLE series GS21 model GS2110-WTBD-N all versions and GOT SIMPLE series GS21 model GS2107-WTBD-N all versions allows a remote unauthenticated attacker to gain unauthorized access via specially crafted packets when the "VNC server" function is used.	2021-04-22	not yet calculated	CVE-2021-20590 CONFIRM CONFIRM
ms-wsp -- wireshark	Excessive memory consumption in MS-WSP dissector in Wireshark 3.4.0 to 3.4.4 and 3.2.0 to 3.2.12 allows denial of service via packet injection or crafted capture file	2021-04-23	not yet calculated	CVE-2021-22207 CONFIRM MISC MISC
nucleus -- multiple_products	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a read access past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition.	2021-04-22	not yet calculated	CVE-2020-27738 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nucleus -- multiple_products	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS response parsing functionality does not properly validate various length and counts of the records. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the memory past the allocated structure.	2021-04-22	not yet calculated	CVE-2020-27737 MISC MISC
nucleus -- multiple_products	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS domain name label parsing functionality does not properly validate the null-terminated name in DNS-responses. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the read memory.	2021-04-22	not yet calculated	CVE-2020-27736 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nucleus -- multiple_products	A vulnerability has been identified in Nucleus NET (All versions < V5.2), Nucleus RTOS (versions including affected DNS modules), Nucleus Source Code (versions including affected DNS modules), VSTAR (versions including affected DNS modules). The DNS domain name record decompression functionality does not properly validate the pointer offset values. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.	2021-04-22	not yet calculated	CVE-2020-27009 MISC MISC
nucleus -- multiple_products	A vulnerability has been identified in Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2013.08), Nucleus Source Code (versions including affected DNS modules), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize UDP port numbers of DNS requests. That could allow an attacker to poison the DNS cache or spoof DNS resolving.	2021-04-22	not yet calculated	CVE-2021-27393 MISC
nucleus -- multiple_products	A vulnerability has been identified in Nucleus NET (All versions < V5.2), Nucleus RTOS (versions including affected DNS modules), Nucleus Source Code (versions including affected DNS modules), VSTAR (versions including affected DNS modules). The DNS domain name label parsing functionality does not properly validate the names in DNS-responses. The parsing of malformed responses could result in a write past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to execute code in the context of the current process or cause a denial-of-service condition.	2021-04-22	not yet calculated	CVE-2020-15795 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nucleus -- nucleus4	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values.	2021-04-22	not yet calculated	CVE-2021-25663 MISC CONFIRM
nucleus -- nucleus4	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving.	2021-04-22	not yet calculated	CVE-2021-25677 MISC MISC
nucleus -- nucleus4	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values.	2021-04-22	not yet calculated	CVE-2021-25664 MISC MISC
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where the program dereferences a pointer that contains a location for memory that is no longer valid, which may lead to code execution, denial of service, or escalation of privileges.	2021-04-21	not yet calculated	CVE-2021-1075 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- windows_gpu_display_driver	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys or nvidia.ko) where improper access control may lead to denial of service, information disclosure, or data corruption.	2021-04-21	not yet calculated	CVE-2021-1076 CONFIRM
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver for Windows, R390 driver branch, contains a vulnerability in its installer where an attacker with local system access may replace an application resource with malicious files. Such an attack may lead to code execution, escalation of privileges, denial of service, or information disclosure.	2021-04-21	not yet calculated	CVE-2021-1074 CONFIRM
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver for Windows, all versions, contains a vulnerability in the kernel driver (nvlddmkm.sys) where a NULL pointer dereference may lead to system crash.	2021-04-21	not yet calculated	CVE-2021-1078 CONFIRM
nvidia -- windows_gpu_display_driver	NVIDIA GPU Display Driver for Windows and Linux, R450 and R460 driver branch, contains a vulnerability where the software uses a reference count to manage a resource that is incorrectly updated, which may lead to denial of service.	2021-04-21	not yet calculated	CVE-2021-1077 CONFIRM
opcenter -- quality_and_qms_automotive	A vulnerability has been identified in Opcenter Quality (All versions < V12.2), QMS Automotive (All versions < V12.30). A private sign key is shipped with the product without adequate protection.	2021-04-22	not yet calculated	CVE-2021-27389 MISC
oracle -- database_server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2234 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- database_server	Vulnerability in the Oracle Database - Enterprise Edition Unified Audit component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Audit Policy privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Unified Audit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition Unified Audit accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2021-04-22	not yet calculated	CVE-2021-2245 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Legal Entity Configurator product of Oracle E-Business Suite (component: Create Contracts). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Legal Entity Configurator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Legal Entity Configurator accessible data as well as unauthorized access to critical data or complete access to all Oracle Legal Entity Configurator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2273 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Site Hub product of Oracle E-Business Suite (component: Sites). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Site Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Site Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Site Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2270 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Sourcing product of Oracle E-Business Suite (component: Intelligence, RFx). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sourcing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sourcing accessible data as well as unauthorized access to critical data or complete access to all Oracle Sourcing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2263 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Endeca). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Purchasing accessible data as well as unauthorized access to critical data or complete access to all Oracle Purchasing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2262 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Lease and Finance Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Lease and Finance Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Lease and Finance Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Lease and Finance Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2261 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: iRecruitment). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2260 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Payables product of Oracle E-Business Suite (component: India Localization, Results). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payables accessible data as well as unauthorized access to critical data or complete access to all Oracle Payables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2259 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Projects product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Projects. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Projects accessible data as well as unauthorized access to critical data or complete access to all Oracle Projects accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2258 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Resource Exceptions). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2271 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Storage Cloud Software Appliance product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 16.3.1.4.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Storage Cloud Software Appliance. While the vulnerability is in Oracle Storage Cloud Software Appliance, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Storage Cloud Software Appliance. Note: Updating the Oracle Storage Cloud Software Appliance to version 16.3.1.4.2 or later will address these vulnerabilities. Download the latest version of Oracle Storage Cloud Software Appliance from <a href="https://us-cert.cisa.gov https://www.oracle.com/downloads/cloud/oscsa-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rstype=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2256 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: APIs). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Installed Base accessible data as well as unauthorized access to critical data or complete access to all Oracle Installed Base accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2231 MISC
oracle -- e-business_suite	Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Process Operations). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle MES for Process Manufacturing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle MES for Process Manufacturing accessible data as well as unauthorized access to critical data or complete access to all Oracle MES for Process Manufacturing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2238 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle E-Business Tax product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle E-Business Tax. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Tax accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Business Tax accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2274 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2275 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSetup accessible data as well as unauthorized access to critical data or complete access to all Oracle iSetup accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2276 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Setup). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Asset Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Asset Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2233 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Account Hierarchy Manager). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2237 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Project Contracts product of Oracle E-Business Suite (component: Hold Management). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Project Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Project Contracts accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2254 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle HRMS (France) product of Oracle E-Business Suite (component: French HR). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle HRMS (France). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HRMS (France) accessible data as well as unauthorized access to critical data or complete access to all Oracle HRMS (France) accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2316 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Engineering product of Oracle E-Business Suite (component: Change Management). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Engineering. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Engineering accessible data as well as unauthorized access to critical data or complete access to all Oracle Engineering accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2290 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Document Management). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Document Management and Collaboration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Document Management and Collaboration accessible data as well as unauthorized access to critical data or complete access to all Oracle Document Management and Collaboration accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2292 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Profiles). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Application Object Library accessible data as well as unauthorized access to critical data or complete access to all Oracle Application Object Library accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2314 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Subledger Accounting product of Oracle E-Business Suite (component: Inquiries). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Subledger Accounting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Subledger Accounting accessible data as well as unauthorized access to critical data or complete access to all Oracle Subledger Accounting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2272 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Bills of Material product of Oracle E-Business Suite (component: Bill Issues). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Bills of Material. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Bills of Material accessible data as well as unauthorized access to critical data or complete access to all Oracle Bills of Material accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2288 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Product Hub product of Oracle E-Business Suite (component: Template, GTIN search). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Product Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Product Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Product Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2289 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Concurrent Processing product of Oracle E-Business Suite (component: BI Publisher Integration). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Concurrent Processing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Concurrent Processing accessible data as well as unauthorized access to critical data or complete access to all Oracle Concurrent Processing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2295 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Advanced Pricing product of Oracle E-Business Suite (component: Price Book). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Pricing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Pricing accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Pricing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2269 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Landed Cost Management product of Oracle E-Business Suite (component: Shipment Workbench). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Landed Cost Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Landed Cost Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Landed Cost Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2249 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Quoting product of Oracle E-Business Suite (component: Courseware). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quoting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Quoting accessible data as well as unauthorized access to critical data or complete access to all Oracle Quoting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2268 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Advanced Collections product of Oracle E-Business Suite (component: Admin). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Collections. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Collections accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Collections accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2247 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Intelligence accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2225 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Bill Presentment Architecture product of Oracle E-Business Suite (component: Template Search). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Bill Presentment Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Bill Presentment Architecture accessible data as well as unauthorized access to critical data or complete access to all Oracle Bill Presentment Architecture accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2222 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2221 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Cash Management product of Oracle E-Business Suite (component: Bank Account Transfer). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cash Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Cash Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Cash Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2227 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Incentive Compensation product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Incentive Compensation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Incentive Compensation accessible data as well as unauthorized access to critical data or complete access to all Oracle Incentive Compensation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2228 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: LOVs). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Depot Repair accessible data as well as unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2229 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Labor Distribution product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Labor Distribution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Labor Distribution accessible data as well as unauthorized access to critical data or complete access to all Oracle Labor Distribution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2267 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Transportation Execution product of Oracle E-Business Suite (component: Install and Upgrade). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Execution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Transportation Execution accessible data as well as unauthorized access to critical data or complete access to all Oracle Transportation Execution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2235 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Financials Common Modules product of Oracle E-Business Suite (component: Advanced Global Intercompany). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials Common Modules. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financials Common Modules accessible data as well as unauthorized access to critical data or complete access to all Oracle Financials Common Modules accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2236 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Time and Labor product of Oracle E-Business Suite (component: Timecard). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Time and Labor. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Time and Labor accessible data as well as unauthorized access to critical data or complete access to all Oracle Time and Labor accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2239 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iStore. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iStore accessible data as well as unauthorized access to critical data or complete access to all Oracle iStore accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2241 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Compensation Workbench product of Oracle E-Business Suite (component: Compensation Workbench). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Compensation Workbench. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Compensation Workbench accessible data as well as unauthorized access to critical data or complete access to all Oracle Compensation Workbench accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2224 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Universal Work Queue accessible data as well as unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2246 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Receivables product of Oracle E-Business Suite (component: Receipts). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Receivables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Receivables accessible data as well as unauthorized access to critical data or complete access to all Oracle Receivables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2223 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle Loans product of Oracle E-Business Suite (component: Loan Details, Loan Accounting Events). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Loans. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Loans accessible data as well as unauthorized access to critical data or complete access to all Oracle Loans accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2252 MISC
oracle -- e-business_suite	Vulnerability in the Oracle Service Contracts product of Oracle E-Business Suite (component: Authoring). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Service Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Service Contracts accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2255 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Data Source). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle CRM Technical Foundation accessible data as well as unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2251 MISC
oracle -- fusion_middelware	Vulnerability in the Oracle Platform Security for Java product of Oracle Fusion Middleware (component: OPSS). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Platform Security for Java. Successful attacks of this vulnerability can result in takeover of Oracle Platform Security for Java. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2302 MISC MISC
oracle -- fusion_middleware	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Coherence accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2277 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- fusion_middleware	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data as well as unauthorized read access to a subset of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	2021-04-22	not yet calculated	CVE-2021-2315 MISC
oracle -- fusion_middleware	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2021-04-22	not yet calculated	CVE-2021-2294 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- fusion_middleware	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2242 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- fusion_middleware	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2021-04-22	not yet calculated	CVE-2021-2240 MISC
oracle -- hospitality_inventory_management	Vulnerability in the Oracle Hospitality Inventory Management product of Oracle Food and Beverage Applications (component: Export to Reporting and Analytics). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Inventory Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Inventory Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2311 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- hyperion	Vulnerability in the Hyperion Analytic Provider Services product of Oracle Hyperion (component: JAPI). Supported versions that are affected are 11.1.2.4 and 12.2.1.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Analytic Provider Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Analytic Provider Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Hyperion Analytic Provider Services. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2244 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	not yet calculated	CVE-2021-2146 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u291, 8u281, 11.0.10, 16; Java SE Embedded: 8u281; Oracle GraalVM Enterprise Edition: 19.3.5, 20.3.1.2 and 21.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2163 MISC MLIST FEDORA FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u291, 8u281, 11.0.10, 16; Java SE Embedded: 8u281; Oracle GraalVM Enterprise Edition: 19.3.5, 20.3.1.2 and 21.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. It can also be exploited by supplying untrusted data to APIs in the specified Component. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2161 MISC MLIST DEBIAN FEDORA FEDORA
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	not yet calculated	CVE-2021-2154 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	not yet calculated	CVE-2021-2166 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2144 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2021-04-22	not yet calculated	CVE-2021-2162 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	not yet calculated	CVE-2021-2160 MISC
oracle -- secure_global_desktop	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via SKID to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2248 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- storage_gateway	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href="https://us-cert.cisa.gov https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2317 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- storage_gateway	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href="https://us-cert.cisa.gov https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2318 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- storage_gateway	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href="https://us-cert.cisa.gov https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2320 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- storage_gateway	Vulnerability in the Oracle Storage Cloud Software Appliance product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 16.3.1.4.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Storage Cloud Software Appliance. While the vulnerability is in Oracle Storage Cloud Software Appliance, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Storage Cloud Software Appliance accessible data. Note: Updating the Oracle Storage Cloud Software Appliance to version 16.3.1.4.2 or later will address these vulnerabilities. Download the latest version of Oracle Storage Cloud Software Appliance from <a href="https://us-cert.cisa.gov https://www.oracle.com/downloads/cloud/oscsa-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rstype=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2257 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- storage_gateway	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a href="https://us-cert.cisa.gov https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html">here. Refer to Document <a href="https://support.oracle.com/rs?type=doc&id=2768897.1">2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2319 MISC
oracle -- supply_chain	Vulnerability in the Oracle Advanced Supply Chain Planning product of Oracle Supply Chain (component: Core). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Supply Chain Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Supply Chain Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Supply Chain Planning accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2253 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- support_tools	Vulnerability in the OSS Support Tools product of Oracle Support Tools (component: Diagnostic Assistant). The supported version that is affected is Prior to 2.12.41. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise OSS Support Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all OSS Support Tools accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2303 MISC MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2264 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-04-22	not yet calculated	CVE-2021-2312 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2291 MISC MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2283 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2285 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2287 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2281 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2310 MISC MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2296 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2250 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2282 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2279 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2284 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2297 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2306 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-04-22	not yet calculated	CVE-2021-2309 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2266 MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2021-04-22	not yet calculated	CVE-2021-2280 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	2021-04-22	not yet calculated	CVE-2021-2286 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-04-22	not yet calculated	CVE-2021-2142 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.1-49141. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the current user on the host system. Was ZDI-CAN-12130.	2021-04-22	not yet calculated	CVE-2021-27278 MISC MISC
peoplesoft -- enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L).	2021-04-22	not yet calculated	CVE-2021-2219 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
peoplesoft -- enterprise_pt_peoplesoft	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Health Center). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L).	2021-04-22	not yet calculated	CVE-2021-2218 MISC
peoplesoft -- enterprise_scm_eprocurement	Vulnerability in the PeopleSoft Enterprise SCM eProcurement product of Oracle PeopleSoft (component: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2021-04-22	not yet calculated	CVE-2021-2220 MISC
prototype_pollution -- prototype_pollution	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in backbone-query-parameters 0.4.0 allows a malicious user to inject properties into Object.prototype.	2021-04-23	not yet calculated	CVE-2021-20085 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
prototype_pollution -- prototype_pollution	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-sparkle 1.5.2-beta allows a malicious user to inject properties into Object.prototype.	2021-04-23	not yet calculated	CVE-2021-20084 MISC
prototype_pollution -- prototype_pollution	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in mootools-more 1.6.0 allows a malicious user to inject properties into Object.prototype.	2021-04-23	not yet calculated	CVE-2021-20088 MISC
prototype_pollution -- prototype_pollution	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-deparam 0.5.1 allows a malicious user to inject properties into Object.prototype.	2021-04-23	not yet calculated	CVE-2021-20087 MISC
prototype_pollution -- prototype_pollution	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-bbq 1.2.1 allows a malicious user to inject properties into Object.prototype.	2021-04-23	not yet calculated	CVE-2021-20086 MISC
prototype_pollution -- prototype_pollution	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in purl 2.3.2 allows a malicious user to inject properties into Object.prototype.	2021-04-23	not yet calculated	CVE-2021-20089 MISC
prototype_pollution -- prototype_pollution	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-plugin-query-object 2.2.3 allows a malicious user to inject properties into Object.prototype.	2021-04-23	not yet calculated	CVE-2021-20083 MISC
pulse_connect_secure -- pulse_connect_secure	Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure that can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway. This vulnerability has been exploited in the wild.	2021-04-23	not yet calculated	CVE-2021-22893 MISC MISC MISC MISC
react-draft-wysiwyg -- react-draft-wysiwyg	react-draft-wysiwyg (aka React Draft Wysiwyg) before 1.14.6 allows a javascript: URi in a Link Target of the link decorator in decorators/Link/index.js when a draft is shared across users, leading to XSS.	2021-04-24	not yet calculated	CVE-2021-31712 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redis -- node-redis	Node-redis is a Node.js Redis client. Before version 3.1.1, when a client is in monitoring mode, the regex begin used to detected monitor messages could cause exponential backtracking on some strings. This issue could lead to a denial of service. The issue is patched in version 3.1.1.	2021-04-23	not yet calculated	CVE-2021-29469 MISC MISC CONFIRM
retdec -- retdec	An issue was discovered in retdec v3.3. In function canSplitFunctionOn() of ir_modifications.cpp, there is a possible out of bounds read due to a heap buffer overflow. The impact is: Deny of Service, Memory Disclosure, and Possible Code Execution.	2021-04-21	not yet calculated	CVE-2020-23907 MISC MISC
ruby -- ruby	The REXML gem before 3.2.5 in Ruby before 2.6.7, 2.7.x before 2.7.3, and 3.x before 3.0.1 does not properly address XML round-trip issues. An incorrect document can be produced after parsing and serializing.	2021-04-21	not yet calculated	CVE-2021-28965 MISC FEDORA
salkstack -- salt	In SaltStack Salt 2016.9 through 3002.6, a command injection vulnerability exists in the snapper module that allows for local privilege escalation on a minion. The attack requires that a file is created with a pathname that is backed up by snapper, and that the master calls the snapper.diff function (which executes popen unsafely).	2021-04-23	not yet calculated	CVE-2021-31607 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
scalance -- multiple_products	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.	2021-04-22	not yet calculated	CVE-2021-25669 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
scalance -- multiple_products	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.	2021-04-22	not yet calculated	CVE-2021-25668 MISC
sipwise -- sipwise	Sipwise C5 NGCP CSC through CE_m39.3.1 allows call/click2dial CSRF attacks for actions with administrative privileges	2021-04-23	not yet calculated	CVE-2021-31584 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sipwise -- sipwise	Sipwise C5 NGCP CSC through CE_m39.3.1 has multiple authenticated stored and reflected XSS vulnerabilities when input passed via several parameters to several scripts is not properly sanitized before being returned to the user: Stored XSS in callforward/time/set/save (POST tsetname); Reflected XSS in addressbook (GET filter); Stored XSS in addressbook/save (POST firstname, lastname, company); and Reflected XSS in statistics/versions (GET lang).	2021-04-23	not yet calculated	CVE-2021-31583 MISC MISC MISC
siveillance -- multiple_products	A vulnerability has been identified in Siveillance Video Open Network Bridge (2020 R3), Siveillance Video Open Network Bridge (2020 R2), Siveillance Video Open Network Bridge (2020 R1), Siveillance Video Open Network Bridge (2019 R3), Siveillance Video Open Network Bridge (2019 R2), Siveillance Video Open Network Bridge (2019 R1), Siveillance Video Open Network Bridge (2018 R3), Siveillance Video Open Network Bridge (2018 R2). Affected Open Network Bridges store user credentials for the authentication between ONVIF clients and ONVIF server using a hard-coded key. The encrypted credentials can be retrieved via the MIP SDK. This could allow an authenticated remote attacker to retrieve and decrypt all credentials stored on the ONVIF server.	2021-04-22	not yet calculated	CVE-2021-27392 MISC
solarwinds -- orion_virtual_infrastructure_monitor	This vulnerability allows local attackers to escalate privileges on affected installations of SolarWinds Orion Virtual Infrastructure Monitor 2020.2. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the OneTimeJobSchedulerEventsService WCF service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-11955.	2021-04-22	not yet calculated	CVE-2021-27277 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solid_edge -- multiple_products	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13040)	2021-04-22	not yet calculated	CVE-2021-27382 MISC CONFIRM
solid_edge -- multiple_products	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could lead to pointer dereferences of a value obtained from untrusted source. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-11919)	2021-04-22	not yet calculated	CVE-2020-26997 MISC MISC
solid_edge -- multiple_products	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12529)	2021-04-22	not yet calculated	CVE-2021-25678 MISC
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3 Pro up to and including 3.30.0 has Incorrect Access Control.	2021-04-23	not yet calculated	CVE-2021-29158 MISC CONFIRM
tecnomatix -- robotexpert	A vulnerability has been identified in Tecnomatix RobotExpert (All versions < V16.1). Affected applications lack proper validation of user-supplied data when parsing CELL files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12608)	2021-04-22	not yet calculated	CVE-2021-25670 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tibco -- multiple_products	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Runtime Agent, TIBCO Runtime Agent, TIBCO Runtime Agent for z/Linux, and TIBCO Runtime Agent for z/Linux contains an easily exploitable vulnerability that allows an unauthenticated attacker to social engineer a legitimate user with network access to execute a Stored XSS attack targeting the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent: versions 5.10.2 and below, TIBCO Runtime Agent: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent for z/Linux: versions 5.10.2 and below, and TIBCO Runtime Agent for z/Linux: versions 5.11.0 and 5.11.1.	2021-04-20	not yet calculated	CVE-2021-28827 CONFIRM CONFIRM
trend_micro -- antivirus	Trend Micro Antivirus for Mac 2020 v10.5 and 2021 v11 (Consumer) is vulnerable to an improper access control privilege escalation vulnerability that could allow an attacker to establish a connection that could lead to full local privilege escalation within the application. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	2021-04-22	not yet calculated	CVE-2021-28648 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
unisys_stealth -- unisys_stealth	Unisys Stealth (core) 5.x before 5.0.048.0, 5.1.x before 5.1.017.0, and 6.x before 6.1.037.0 stores Passwords in a Recoverable Format.	2021-04-20	not yet calculated	CVE-2021-28492 MISC CONFIRM
upnp -- multiple_devices	The Portable SDK for UPnP Devices is an SDK for development of UPnP device and control point applications. The server part of pupnp (libupnp) appears to be vulnerable to DNS rebinding attacks because it does not check the value of the `Host` header. This can be mitigated by using DNS revolvers which block DNS-rebinding attacks. The vulnerability is fixed in version 1.14.6 and later.	2021-04-20	not yet calculated	CVE-2021-29462 CONFIRM MLIST
vaadin -- vaadin	Non-constant-time comparison of CSRF tokens in endpoint request handler in com.vaadin:flow-server versions 3.0.0 through 5.0.3 (Vaadin 15.0.0 through 18.0.6), and com.vaadin:fusion-endpoint version 6.0.0 (Vaadin 19.0.0) allows attacker to guess a security token for Fusion endpoints via timing attack.	2021-04-23	not yet calculated	CVE-2021-31406 CONFIRM CONFIRM
vaadin -- vaadin	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.13 (Vaadin 10.0.0 through 10.0.16), 1.1.0 prior to 2.0.0 (Vaadin 11 prior to 14), 2.0.0 through 2.4.6 (Vaadin 14.0.0 through 14.4.6), 3.0.0 prior to 5.0.0 (Vaadin 15 prior to 18), and 5.0.0 through 5.0.2 (Vaadin 18.0.0 through 18.0.5) allows attacker to guess a security token via timing attack.	2021-04-23	not yet calculated	CVE-2021-31404 CONFIRM CONFIRM
vaadin -- vaadin	Authentication.logout() helper in com.vaadin:flow-client versions 5.0.0 prior to 6.0.0 (Vaadin 18), and 6.0.0 through 6.0.4 (Vaadin 19.0.0 through 19.0.3) uses incorrect HTTP method, which, in combination with Spring Security CSRF protection, allows local attackers to access Fusion endpoints after the user attempted to log out.	2021-04-23	not yet calculated	CVE-2021-31408 MISC MISC
vaadin -- vaadin	Missing variable sanitization in Grid component in com.vaadin:vaadin-server versions 7.4.0 through 7.7.19 (Vaadin 7.4.0 through 7.7.19), and 8.0.0 through 8.8.4 (Vaadin 8.0.0 through 8.8.4) allows attacker to inject malicious JavaScript via unspecified vector	2021-04-23	not yet calculated	CVE-2019-25028 CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vaadin -- vaadin	Insecure configuration of default ObjectMapper in com.vaadin:flow-server versions 3.0.0 through 3.0.5 (Vaadin 15.0.0 through 15.0.4) may expose sensitive data if the application also uses e.g. @RestController	2021-04-23	not yet calculated	CVE-2020-36319 CONFIRM CONFIRM CONFIRM
vaadin -- vaadin	Overly relaxed configuration of frontend resources server in Vaadin Designer versions 4.3.0 through 4.6.3 allows remote attackers to access project sources via crafted HTTP request.	2021-04-23	not yet calculated	CVE-2021-31410 MISC
vaadin -- vaadin	Unsafe validation RegEx in EmailValidator class in com.vaadin:vaadin-server versions 7.0.0 through 7.7.21 (Vaadin 7.0.0 through 7.7.21) allows attackers to cause uncontrolled resource consumption by submitting malicious email addresses.	2021-04-23	not yet calculated	CVE-2020-36320 CONFIRM CONFIRM CONFIRM
vaadin -- vaadin	Improper URL validation in development mode handler in com.vaadin:flow-server versions 2.0.0 through 2.4.1 (Vaadin 14.0.0 through 14.4.2), and 3.0 prior to 5.0 (Vaadin 15 prior to 18) allows attacker to request arbitrary files stored outside of intended frontend resources folder.	2021-04-23	not yet calculated	CVE-2020-36321 CONFIRM CONFIRM
vaadin -- vaadin	Vulnerability in OSGi integration in com.vaadin:flow-server versions 1.2.0 through 2.4.7 (Vaadin 12.0.0 through 14.4.9), and 6.0.0 through 6.0.1 (Vaadin 19.0.0) allows attacker to access application classes and resources on the server via crafted HTTP request.	2021-04-23	not yet calculated	CVE-2021-31407 CONFIRM CONFIRM CONFIRM CONFIRM
vaadin -- vaadin	Missing check in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.5 (Vaadin 10.0.0 through 10.0.7, and 11.0.0 through 11.0.2) allows attacker to update element property values via crafted synchronization message.	2021-04-23	not yet calculated	CVE-2018-25007 CONFIRM CONFIRM
vaadin -- vaadin	Unsafe validation RegEx in EmailField component in com.vaadin:vaadin-text-field-flow versions 2.0.4 through 2.3.2 (Vaadin 14.0.6 through 14.4.3), and 3.0.0 through 4.0.2 (Vaadin 15.0.0 through 17.0.10) allows attackers to cause uncontrolled resource consumption by submitting malicious email addresses.	2021-04-23	not yet calculated	CVE-2021-31405 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vaadin -- vaadin	Missing output sanitization in default RouteNotFoundError view in com.vaadin:flow-server versions 1.0.0 through 1.0.10 (Vaadin 10.0.0 through 10.0.13), and 1.1.0 through 1.4.2 (Vaadin 11.0.0 through 13.0.5) allows attacker to execute malicious JavaScript via crafted URL	2021-04-23	not yet calculated	CVE-2019-25027 CONFIRM CONFIRM
vaadin -- vaadin	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:vaadin-server versions 7.0.0 through 7.7.23 (Vaadin 7.0.0 through 7.7.23), and 8.0.0 through 8.12.2 (Vaadin 8.0.0 through 8.12.2) allows attacker to guess a security token via timing attack	2021-04-23	not yet calculated	CVE-2021-31403 CONFIRM CONFIRM CONFIRM
void -- aural_rec_monitor	An issue was discovered in svc-login.php in Void Aural Rec Monitor 9.0.0.1. Passwords are stored in unencrypted source-code text files. This was noted when accessing the svc-login.php file. The value is used to authenticate a high-privileged user upon authenticating with the server.	2021-04-23	not yet calculated	CVE-2021-25898 MISC MISC
void -- aural_rec_monitor	An issue was discovered in svc-login.php in Void Aural Rec Monitor 9.0.0.1. An unauthenticated attacker can send a crafted HTTP request to perform a blind time-based SQL Injection. The vulnerable parameter is param1.	2021-04-23	not yet calculated	CVE-2021-25899 MISC MISC
wikimedia -- quarry	Wikimedia Quarry analytics-quarry-web before 2020-12-15 allows Reflected XSS because app.py does not explicitly set the application/json content type.	2021-04-21	not yet calculated	CVE-2020-36324 MISC MISC
wordpress -- wordpress	The Pie Register â€“ User Registration Forms. Invitation based registrations, Custom Login, Payments WordPress plugin before 3.7.0.1 does not sanitise the invitaion_code GET parameter when outputting it in the Activation Code page, leading to a reflected Cross-Site Scripting issue.	2021-04-22	not yet calculated	CVE-2021-24239 CONFIRM MISC
wordpress -- wordpress	An improper authorization of using debugging command in Secure Folder prior to SMR Oct-2020 Release 1 allows unauthorized access to contents in Secure Folder via debugging command.	2021-04-23	not yet calculated	CVE-2021-25382 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Cooked Pro WordPress plugin before 1.7.5.6 was affected by unauthenticated reflected Cross-Site Scripting issues, due to improper sanitisation of user input while being output back in pages as an arbitrary attribute.	2021-04-22	not yet calculated	CVE-2021-24233 MISC CONFIRM MISC
wordpress -- wordpress	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not ensure that the requested property to be deleted belong to the user making the request, allowing any authenticated users to delete arbitrary properties by tampering with the property_id parameter.	2021-04-22	not yet calculated	CVE-2021-24238 CONFIRM MISC MISC MISC
wordpress -- wordpress	The Goto WordPress theme before 2.0 does not sanitise the keywords and start_date GET parameter on its Tour List page, leading to an unauthenticated reflected Cross-Site Scripting issue.	2021-04-22	not yet calculated	CVE-2021-24235 CONFIRM MISC
wordpress -- wordpress	The Search Forms page of the Ivory Search WordPress lugin before 4.6.1 did not properly sanitise the tab parameter before output it in the page, leading to a reflected Cross-Site Scripting issue when opening a malicious crafted link as a high privilege user. Knowledge of a form id is required to conduct the attack.	2021-04-22	not yet calculated	CVE-2021-24234 MISC MISC CONFIRM
wordpress -- wordpress	The Tutor LMS â€“ eLearning and online course solution WordPress plugin before 1.8.8 is affected by a local file inclusion vulnerability through the maliciously constructed sub_page parameter of the plugin's Tools, allowing high privilege users to include any local php file	2021-04-22	not yet calculated	CVE-2021-24242 CONFIRM
wordpress -- wordpress	The Advanced Custom Fields Pro WordPress plugin before 5.9.1 did not properly escape the generated update URL when outputting it in an attribute, leading to a reflected Cross-Site Scripting issue in the update settings page.	2021-04-22	not yet calculated	CVE-2021-24241 MISC CONFIRM MISC
wordpress -- wordpress	The Advanced Booking Calendar WordPress plugin before 1.6.8 does not sanitise the license error message when output in the settings page, leading to an authenticated reflected Cross-Site Scripting issue	2021-04-22	not yet calculated	CVE-2021-24232 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Business Hours Pro WordPress plugin through 5.5.0 allows a remote attacker to upload arbitrary files using its manual update functionality, leading to an unauthenticated remote code execution vulnerability.	2021-04-22	not yet calculated	CVE-2021-24240 CONFIRM MISC
wordpress -- wordpress	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not properly sanitise the keyword_search, search_radius. _bedrooms and _bathrooms GET parameters before outputting them in its properties page, leading to an unauthenticated reflected Cross-Site Scripting issue.	2021-04-22	not yet calculated	CVE-2021-24237 CONFIRM MISC MISC MISC
wowza -- streaming_engine	Wowza Streaming Engine through 4.8.5 (in a default installation) has cleartext passwords stored in the conf/admin.password file. A regular local user is able to read usernames and passwords.	2021-04-23	not yet calculated	CVE-2021-31539 MISC MISC
wowza -- streaming_engine	Wowza Streaming Engine through 4.8.5 (in a default installation) has incorrect file permissions of configuration files in the conf/ directory. A regular local user is able to read and write to all the configuration files, e.g., modify the application server configuration.	2021-04-23	not yet calculated	CVE-2021-31540 MISC MISC
wrongthink -- wrongthink	Wrongthink is an encrypted peer-to-peer chat program. A user could check their fingerprint into the service and enter a script to run arbitrary JavaScript on the site. No workarounds exist, but a patch exists in version 2.4.1.	2021-04-22	not yet calculated	CVE-2021-29467 CONFIRM
xmlhttprequest -- xmlhttprequest	The xmlhttprequest-ssl package before 1.6.1 for Node.js disables SSL certificate validation by default, because rejectUnauthorized (when the property exists but is undefined) is considered to be false within the https.request function of Node.js. In other words, no certificate is ever rejected.	2021-04-23	not yet calculated	CVE-2021-31597 MISC MISC MISC
xplatform -- xplatform	A vulnerability of XPlatform could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient validation of improper classes. This issue affects: Tobesoft XPlatform versions prior to 9.2.2.280.	2021-04-20	not yet calculated	CVE-2020-7857 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki_platform -- xwiki_platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible to persistently inject scripts in XWiki versions prior to 12.6.3 and 12.8. Unregistred users can fill simple text fields. Registered users can fill in their personal information and (if they have edit rights) fill the values of static lists using App Within Minutes. There is no easy workaround except upgrading XWiki. The vulnerability has been patched on XWiki 12.8 and 12.6.3.	2021-04-20	not yet calculated	CVE-2021-29459 CONFIRM
zoho -- manageengine_opmanager	Zoho ManageEngine OpManager before 12.5.329 allows unauthenticated Remote Code Execution due to a general bypass in the deserialization class.	2021-04-22	not yet calculated	CVE-2021-3287 MISC

Back to top